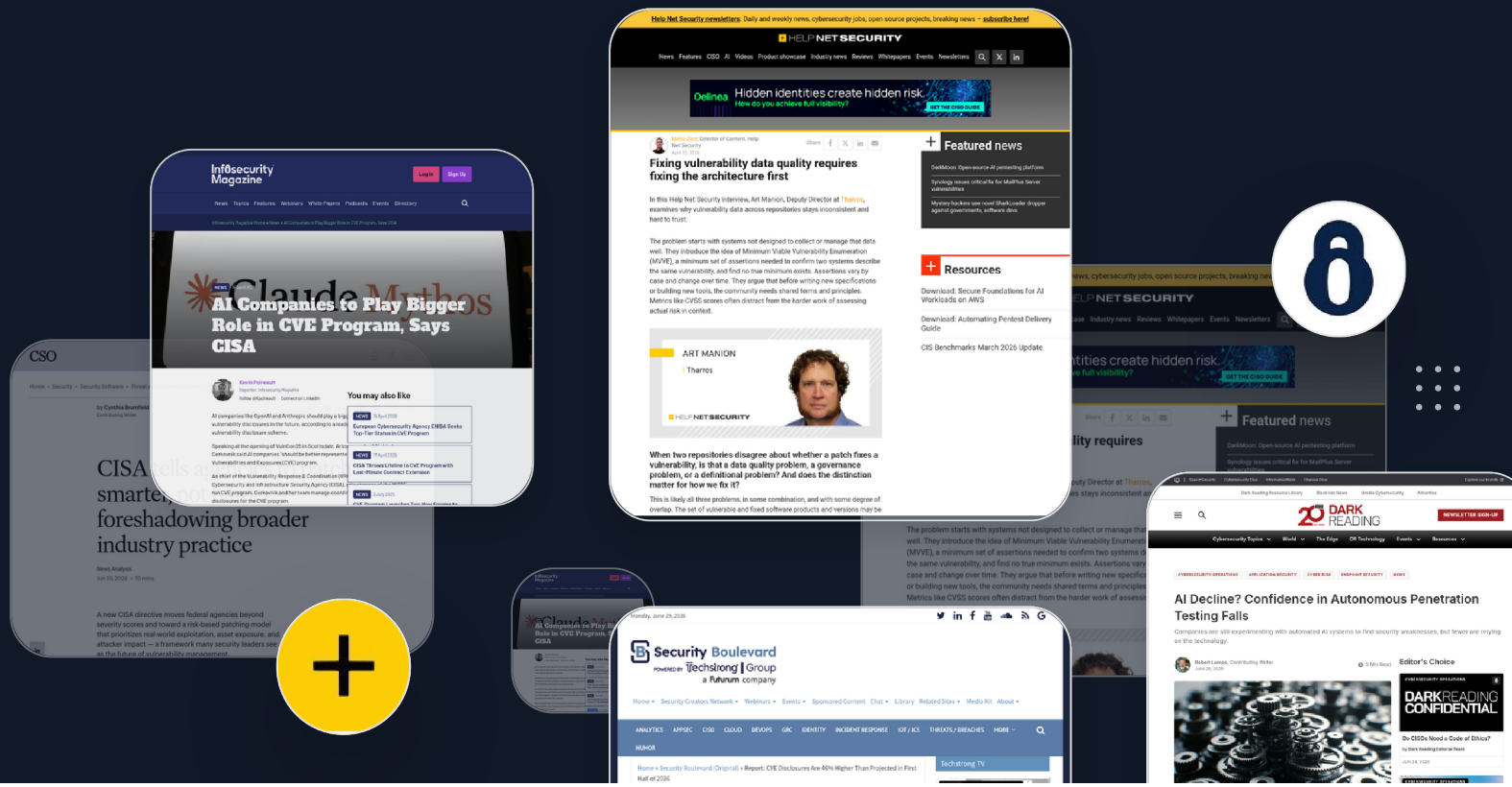




FIRST Q2FY26 PR Coverage (As of 6.29.26)

Presented by Growth Stack Media



Contents

Summary Page **3**

Highlights Page **5**

Coverage Page **7**

Summary



107

Pieces of Coverage

Total number of online, offline and social clips in this report



89.4M

Audience

Combined total of publication-wide audience figures for all outlets featuring coverage



571K

Estimated Views

Prediction of lifetime views of coverage, based on audience reach & engagement rate on...



333

Engagements

Combined total of likes, comments and shares on social media platforms



43

Avg. Domain Authority

A 0-100 measure of the authority of the site coverage appears on. Provided by Moz

Highlights

Help Net Security newsletters Daily and weekly news, cybersecurity jobs, open source projects, breaking news - subscribe

HELP NET SECURITY

News Features CSO AI Videos Product showcase Industry news Reviews Whitepapers Events Newsletters

Oelinea Hidden identities create hidden risk
How do you achieve full visibility? GET THE CSO GUIDE

Mirko Zorc, Director of Content, Help Net Security
April 13, 2026

Fixing vulnerability data quality requires fixing the architecture first

In this Help Net Security interview, Art Marion, Deputy Director at Tharros, examines why vulnerability data across repositories stays inconsistent and hard to trust.

The problem starts with systems not designed to collect or manage that data well. They introduce the idea of Minimum Viable Vulnerability Enumeration (MVVE), a minimum set of assertions needed to confirm two systems describe the same vulnerability, and find no true minimum exists. Assertions vary by case and change over time. They argue that before writing new specifications or building new tools, the community needs shared terms and principles. Metrics like CVSS scores often distract from the harder work of assessing actual risk in context.

Featured news

DarkMoon: Open source AI pentesting platform
Synology issues critical fix for MailPlus Server vulnerabilities
Mystery hackers use novel SharkLoader dropper against governments, software devs

Resources

Download: Secure Foundations for AI Workloads on AWS

Help Net Security

Fixing vulnerability data quality requires fixing the architecture first - Help Net Security

209K 76 1.28K 9

Infosecurity Magazine

Log In Sign Up

News Topics Features Webinars White Papers Podcasts Events Directory

Infosecurity Magazine Home • News • AI Companies to Play Bigger Role in CVE Program, Says CISA

AI Companies to Play Bigger Role in CVE Program, Says CISA

Kevin Poireault
Reporter, Infosecurity Magazine
Follow @Kpoireault Connect on LinkedIn

You may also like

Infosecurity Magazine

AI Companies To Play Bigger Role in CVE Program, Says CISA

109K 71 843 14

SearchSecurity Cybersecurity Dive InformationWeek Channel Dive Explore

Dark Reading Resource Library Black Hat News Omdia Cybersecurity Advertise

20 DARK READING

NEWSLETTER SIGN UP

Cybersecurity Topics World The Edge DR Technology Events Resources

CYBERSECURITY OPERATIONS APPLICATION SECURITY CYBER RISK ENDPOINT SECURITY NEWS

AI Decline? Confidence in Autonomous Penetration Testing Falls

Companies are still experimenting with automated AI systems to find security weaknesses, but fewer are relying on the technology.

Robert Lemos, Contributing Writer
June 26, 2026

5 Min Read Editor's Choice

DARK READING CONFIDENTIAL

Dark Reading

AI Decline? Confidence Falls in Autonomous Penetration Testing

194K 82 933

Monday, June 29, 2026

Security Boulevard
POWERED BY Techstrong Group
a Futurum company

Home • Security Creators Network • Webinars • Events • Sponsored Content • Chat • Library Related Sites • Media Kit About

ANALYTICS APPSEC CSO CLOUD DEVOPS GRC IDENTITY INCIDENT RESPONSE IoT/ICS THREATS/BREACHES MORE

HUMOR

Home • Security Boulevard (Original) • Report: CVE Disclosures Are 46% Higher Than Projected in First Half of 2026

Report: CVE Disclosures Are 46% Higher Than Projected in First Half of 2026

By Michael Vizard on June 22, 2026

A report published by the Forum of Incident Response and Security Teams (FIRST), a nonprofit organization for incident response professionals, finds that the rate at which Common Vulnerabilities and Exposures (CVE) are being disclosed in the first half of 2026 is 46% higher than initially projected.

FIRST is now projecting there will be approximately 66,000 CVEs disclosed in 2026, up from the 59,427 that were initially forecasted in February.

Erinann Leventoff, lead member of the vulnerability forensic team at FIRST, said it's not possible to

Techstrong TV

LIVE Unmute broadcast

Click full screen to enable volume control
Watch latest episodes and shows

Tech Field Day Events

Security Boulevard

Report: CVE Disclosures Are 46% Higher Than Projected in First Half of 2026

71.5K 70 533

CSO

Home • Security • Security Software • Threat and Vulnerability Management

by Cynthia Brunfield
Contributing Writer

CISA tells agencies to patch smarter, not harder — foreshadowing broader industry practice

News Analysis
Jun 10, 2026 • 10 mins

A new CISA directive moves federal agencies beyond

CSO Online

CISA tells agencies to patch smarter, not harder — foreshadowing broader industry practice

165K 84 678 6

Coverage

107 pieces



Help Net Security

Cybersecurity news with a focus on enterprise security. Discover what matters in the world of...

76

Domain
Authority ?

Provided by
MOZ

209K

Unique
Visits ?

Provided by
SimilarWeb

Help Net Security newsletters: Daily and weekly news, cybersecurity jobs, open source projects, breaking news – [subscribe here!](#)

HELPNETSECURITY

News Features CISO AI Videos Product showcase Industry news Reviews Whitepapers Events Newsletters 🔍 X in

Delinea Hidden identities create hidden risk. How do you achieve full visibility? [GET THE CISO GUIDE](#)

 **Mirko Zorz**, Director of Content, Help Net Security
April 7, 2026

Share f X in

The case for fixing CWE weakness patterns instead of patching one bug at a time

In this Help Net Security interview, Alec Summers, [MITRE](#) CVE/CWE Project Lead, discusses how CWE is moving from a background reference into active use in vulnerability disclosure. More CVE records now include CWE mappings from CNAs, which tends to produce more precise root-cause data.

Automation tools help analysts map weaknesses faster, but can reinforce bad patterns if trained on poor examples. Summers argues that fixing weakness patterns reduces recurring work for security teams, even those operating on tight budgets. The core problem is framing: the industry defaults to vulnerability language, while CWE asks teams to focus on what made the bad outcome possible in the first place.

ALEC SUMMERS
MITRE



HELPNETSECURITY

CWE has long existed as a reference taxonomy that many practitioners acknowledged but few actively used. For engineers who have been filing CVEs and ignoring CWE IDs for years, what has changed to make the taxonomy feel relevant to daily work?

CWE has long been embedded in how many organizations approach software development via its prevalence in static analysis tools, secure coding guidance,

Featured news

- DarkMoon: Open-source AI pentesting platform
- Synology issues critical fix for MailPlus Server vulnerabilities
- Mystery hackers use novel SharkLoader dropper against governments, software devs

Resources

- Download: Secure Foundations for AI Workloads on AWS
- Download: Automating Pentest Delivery Guide
- CIS Benchmarks March 2026 Update

Apr 07, 2026 · ONLINE

Interview

The case for fixing CWE weakness patterns instead of...

helpnetsecurity.com/2026/04/07/alec-su...

Estimated Views

1.28K

Engagements

8



プレスリリース・ニュースリリース配信シェアNo.1 | PR TIMES

プレスリリースをPR TIMESで配信して、効果的なPRを実現。上場企業の63.9%(2,585社／4,045社)...

92
Domain Authority
Provided by MOZ

32.1M
Unique Visits
Provided by SimilarWeb

Apr 07, 2026 · ONLINE

フューチャー、脆弱性管理分野のトップカンファレンス...

prtimes.jp/main/html/rd/p/000000825.00...

PR TIMES プレスリリース・ニュースリリース配信サービスのPR TIMES

プレスリリースを受信 企業登録申請 ログイン

Top | テクノロジー | モバイル | アプリ | エンタメ | ビューティー | ファッション | ライフスタイル | ビジネス | グルメ | スポーツ

フューチャー株式会社

会社概要 プレスリリース ストーリー フォロー

フューチャー、脆弱性管理分野のトップカンファレンス「Vulncon2026」に登壇

約1万6千件のOSS分析から見えた「隠れたEOL」の脅威と対策を発表

フューチャー株式会社 2026年4月7日 13時00分



フューチャー株式会社（東京都品川区、代表取締役社長 谷口友彦、以下フューチャー）に所属するサイバーセキュリティノベーショングループ シニアアーキテクト神戸康多と、シニアコンサルタント棚井龍之介が、米国アリゾナ州で開催されるサイバーセキュリティ・脆弱性管理分野のトップカンファレンス「Vulncon 2026」のCall for Speakers（公募発表）に採択され、2026年4月16日（現地）に研究成果を発表することをお知らせします。

「Vulncon」は、サイバーセキュリティの国際標準を推進する非営利団体FIRST（Forum of Incident Response and Security Teams）と、脆弱性の共通識別子を管理するCVE Programが共同開催する国際カンファレンスです。脆弱性管理を中心とした様々なセキュリティ分野の専門家や、政府機関、企業の経営層が一堂に会して議論を行う、サイバーセキュリティ分野でもっとも権威のある国際会議のひとつとして開催されます。

近年、ソフトウェアサプライチェーンを狙ったサイバー攻撃が増加しています。最近でも、CI/CD環境で広く利用されている著名なオープンソースのセキュリティツールがサプライチェーン攻撃の標的となり、認証情報が直接狙われるインシデントが発生しました。こうした事態は、多くの開発現場が依存するOSSの信頼性を根本から揺るがすものであり、OSSの依存関係における適切な管理と継続的な監視がこれまで以上に求められています。本発表では、こうした脅威に実践的に対処するためのアプローチを提示します。

■発表内容

The CVE Blind Spot: Defeating “Hidden EOLs” and Repo Jacking with Engineering Triage & Code Diet
（CVEの死角 〜トリアージと「コードダイエット」で打ち勝つ「隠れたEOL」とリポジトリジャッキングの脅威〜）

現在、標準的な脆弱性管理は共通脆弱性識別子CVE（Common Vulnerabilities and Exposures）の情報に大きく依存しています。当日は、CVEによる管理の「死角」として、EOL（End of Life / 提供やサポート、メンテナンスの終了）を迎えるOSSコンポーネントの危険性について発表します。実稼働環境で稼働中のOSSコンポーネント約1万6千件についてフューチャーが独自に分析した結果、約10%が公式にEOL

Estimated Views

61.7K

Engagements

1



Rivista Cybersecurity Trends

Leggi di più

16

Domain
Authority [?]

Provided by
MOZ

2.04K

Unique
Visits [?]

Provided by
SimilarWeb

Apr 09, 2026

ONLINE

Roundup

Cyber Security Events 2026: la nostra Guida - Rivista...

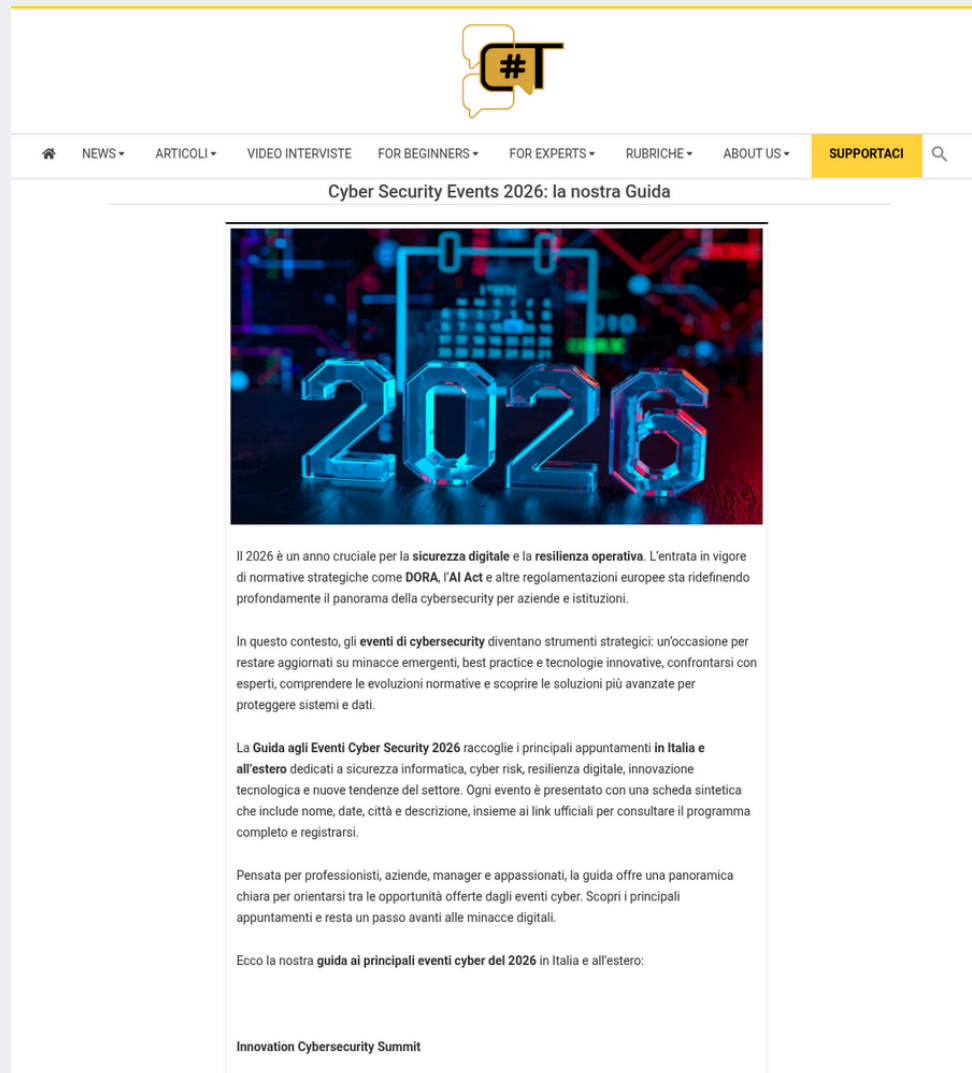
cybertrends.it/cyber-security-events-2026/

Estimated Views

1.09K

Engagements

2





Volerion

We share practical insights from real-world vulnerability data work, including analysis, implementation lessons, and observations that...

13

Domain
Authority [?]

Provided by
MOZ

Apr 13, 2026 · ONLINE

News

Introducing the Volerion Vulnerability Intelligence Platform

blog.volerion.com/posts/introducing-the-v...

Complete CVE enrichment without changing your NVD integration. [Get started](#)

Volerion [Home](#) [About](#) [Posts](#)

Introducing the Volerion Vulnerability Intelligence Platform

Ruben Bos 13 Apr, 2026 Product , Announcements

Most vulnerability dashboards are not effective for daily use. They start promising but quickly become a source of noise. Analysts end up manually checking data instead of making decisions. The problem is not the dashboard itself, but the incomplete data it runs on.

Today, we are introducing the **Volerion Vulnerability Intelligence Platform** beta. It is a practical system to turn vulnerability data into decisions at scale. The dashboard is available at app.volerion.com.

OVERVIEW

[Home](#)

VULNERABILITIES

Index

General

IN

Social Media

Personal Patch List

Create new

Query

STATISTICS

Daily Briefing

Forecast

SOLUTIONS

NVD API

Search in Personal Patch List

Evaluated in the last 7 days (336 CVEs)

Created in the last 7 days (336 CVEs)

☒	☒	CVE-2025-53005	NVIDIA GENOC Unauthenticated Remote Code Execution Vulnerability via Flock Deserialisation - A remote code execu...	Jun 17, 2026
☒	☒	CVE-2025-20190	Close ISE and ISE-PIC Information Disclosure Vulnerability - An information disclosure vulnerability has been ident...	Jun 17, 2026
☒	☒	CVE-2025-18023	Isarth Sentry Authentication Bypass Vulnerability Allowing Creation of Administrative Accounts - A vulnerability allow...	Jun 9, 2026
☒	☒	CVE-2025-18020	Isarth Sentry OS Command Injection Vulnerability Allowing Root-Level Remote Code Execution - A command injecti...	Jun 9, 2026

[Decision log](#) [Integer log](#)

Built on Complete CVE Intelligence

Most vulnerability dashboards look polished, but many run on incomplete or incorrect data. That creates noise for security teams and forces analysts to keep verifying records by hand. We took a different approach at Volerion. We fixed the data problem first by analyzing each and every CVE in-house and filling gaps when public records miss details like CPEs or CVSS scores. Only after that did we build the



Help Net Security

Cybersecurity news with a focus on enterprise security. Discover what matters in the world of...

76

Domain
Authority ?

Provided by
MOZ

209K

Unique
Visits ?

Provided by
SimilarWeb

Help Net Security newsletters: Daily and weekly news, cybersecurity jobs, open source projects, breaking news – [subscribe here!](#)

HELP NET SECURITY

News Features CISO AI Videos Product showcase Industry news Reviews Whitepapers Events Newsletters

Delinea Hidden identities create hidden risk. How do you achieve full visibility? [GET THE CISO GUIDE](#)

Mirko Zorz, Director of Content, Help Net Security
April 13, 2026

Share

Fixing vulnerability data quality requires fixing the architecture first

In this Help Net Security interview, Art Manion, Deputy Director at **Tharros**, examines why vulnerability data across repositories stays inconsistent and hard to trust.

The problem starts with systems not designed to collect or manage that data well. They introduce the idea of Minimum Viable Vulnerability Enumeration (MVVE), a minimum set of assertions needed to confirm two systems describe the same vulnerability, and find no true minimum exists. Assertions vary by case and change over time. They argue that before writing new specifications or building new tools, the community needs shared terms and principles. Metrics like CVSS scores often distract from the harder work of assessing actual risk in context.

ART MANION
Tharros

HELP NET SECURITY

When two repositories disagree about whether a patch fixes a vulnerability, is that a data quality problem, a governance problem, or a definitional problem? And does the distinction matter for how we fix it?

This is likely all three problems, in some combination, and with some degree of overlap. The set of vulnerable and fixed software products and versions may be

Featured news

- DarkMoon: Open-source AI pentesting platform
- Synology issues critical fix for MailPlus Server vulnerabilities
- Mystery hackers use novel SharkLoader dropper against governments, software devs

Resources

- Download: Secure Foundations for AI Workloads on AWS
- Download: Automating Pentest Delivery Guide
- CIS Benchmarks March 2026 Update

Apr 13, 2026

ONLINE

Interview

Fixing vulnerability data quality requires fixing the architectu...

helpnetsecurity.com/2026/04/13/art-manion-interview-fixing-vulnerability-data-quality-requires-fixing-the-architecture-first/

Estimated Views

1.28K

Engagements

9



Infosecurity Magazine

The award winning online magazine dedicated to the strategy, insight and technology of information...

71

Domain Authority ?

Provided by MOZ

109K

Unique Visits ?

Provided by SimilarWeb

The screenshot shows the Infosec Magazine website. The header includes the logo, navigation links (News, Topics, Features, Webinars, White Papers, Podcasts, Events, Directory), and a search bar. The main article is titled "AI Companies to Play Bigger Role in CVE Program, Says CISA" by Kevin Poireault, dated 15 April 2026. The article text is partially visible, discussing the role of AI companies in the CVE program. A sidebar on the right titled "You may also like" lists related articles.

Kevin Poireault
Reporter, Infosecurity Magazine
Follow @Kpoireault Connect on LinkedIn

You may also like

- NEWS** 15 April 2026
European Cybersecurity Agency ENISA Seeks Top-Tier Status in CVE Program
- NEWS** 17 April 2025
CISA Throws Lifeline to CVE Program with Last-Minute Contract Extension
- NEWS** 3 July 2025
CVE Program Launches Two New Forums to Enhance CVE Utilization
- INTERVIEW** 17 April 2026
FIRST CEO Calls for Global CVE Collaboration amid AI Vulnerability Tsunami

Apr 15, 2026 · ONLINE

News

AI Companies To Play Bigger Role in CVE Program, Says CISA

infosecurity-magazine.com/news/ai-comp...

Estimated Views

843

Engagements

14



Team IT Security

Cybersecurity Information Technology Portal von Team IT Security

29

Domain
Authority [?]

Provided by
MOZ

Apr 06, 2026 · ONLINE

Startseite

tsecurity.de/de/3435015/IT+Sicherheit/Cy...

 German

Global Search

Seek

00:13:37

Menu



TSecurity.de

Cybersecurity news. Clear. Fast. Independent.

[News](#) [Security alerts \(EU\)](#) [Security alerts \(USA\)](#) [Latest news by topic](#) [Recent searches](#)

Smartphone: Menu bug fixed | More content added.

Welcome to TSecurity.de

Welcome to TSecurity.de, your **cybersecurity information technology portal**. Here you will find the latest news, tips, videos and downloads daily on **cybersecurity, IT security, operating systems, data protection and more**.

The goal of Team IT Security is to promote IT security and awareness in Germany and beyond.

The "Team IT Security" project, also known as "TSEC," from tsecurity.de aims to provide IT security experts and enthusiasts with information and resources to help them cope with cyber threats.

Newsletter Sign-up

How does newsletter registration work?

How does the newsletter unsubscribe process work?

Nickname or name

Nickname or name...

Email Address

Email Address...

☐ I'm not a robot 

Subscribe to our newsletter

Category



TipRanks | Stock Market Research, News and Analyst Forecasts - TipRanks.com

TipRanks stock market research and analysis, lets
you see the track record and measured...

63

Domain
Authority ⓘ

Provided by
MOZ

3.58M

Unique
Visits ⓘ

Provided by
SimilarWeb

Apr 15, 2026 ·  ONLINE

NetRise Showcases Software Supply Chain Risk...

tipranks.com/news/private-companies/ne...

Estimated Views

38K



We are Tech

We Are Tech met en lumière l'impact de la technologie sur le développement humain et la...

36

Domain
Authority ?

Provided by
MOZ

32.4K

Unique
Visits ?

Provided by
SimilarWeb

Apr 15, 2026 · ONLINE

Mozambique Deepens Cybersecurity Push...

wearetech.africa/en/fils-uk/news/public-m...

Estimated Views

8.2K



Africa Business Insight

Africa Business Insight delivers real-time news, in-depth business analysis, economic trends, and tec...

12

Domain
Authority ?

Provided by
MOZ

314

Unique
Visits ?

Provided by
SimilarWeb

Apr 15, 2026 · ONLINE

News

Mozambique expands cybersecurity capacity through EU...

africabusinessinsight.com/mozambique-e...

Estimated Views

100

Engagements

1

[Home](#) [Business](#) [Finance](#) [Economy](#) [News](#) [Technology](#) [Opinion](#)

Podcast

9.14 \$14.45

NYSE Composite Index \$23,675.86 \$13.38

NASDAQ Composite \$25,605.08 \$307.46

S&P 500 \$7,403.12 \$49.10

FTSE 100 \$13,845.11

BUSINESS

Mozambique expands cybersecurity capacity through EU partnership

Nana Oye Ankras · April 15, 2026 · Africa

Mozambique is accelerating efforts to strengthen its national [cybersecurity](#) architecture through a new cooperation programme with the European Union, aimed at improving technical capacity.

SHARE

Most Read //

1

Kenya seeks \$260 million in market funding to cover budget shortfall

2

Nigeria Super Eagles boycott training ahead of CAF play-offs

3

China leads Chad's US\$4.5 billion oil revival with major



Help Net Security

Cybersecurity news with a focus on enterprise security. Discover what matters in the world of...

76

Domain
Authority ?

Provided by
MOZ

209K

Unique
Visits ?

Provided by
SimilarWeb

Help Net Security newsletters: Daily and weekly news, cybersecurity jobs, open source projects, breaking news – [subscribe here!](#)

HELP NET SECURITY

News Features CISO AI Videos Product showcase Industry news Reviews Whitepapers Events Newsletters

Delinea Hidden identities create hidden risk. How do you achieve full visibility? [GET THE CISO GUIDE](#)

Mirko Zorz, Director of Content, Help Net Security
April 15, 2026

Share

Coordinated vulnerability disclosure is now an EU obligation, but cultural change takes time

In this Help Net Security interview, Nuno Rodrigues Carvalho, Head of Sector for Incident and Vulnerability Services at **ENISA**, discusses the recent **CVE funding scare** and what it exposed about the fragility of global vulnerability disclosure infrastructure. He outlines how EU regulations, including the Cyber Resilience Act and NIS2, are creating stronger accountability for vendors and organizations.

ENISA is building out European vulnerability services to support member states. Carvalho also addresses how practitioners navigate conflicting enrichment sources, and argues the CVE program needs a distributed model with no single point of failure.

NUNO RODRIGUES CARVALHO
| ENISA

HELP NET SECURITY

The CVE program recently experienced a significant funding scare when MITRE's contract with CISA came close to lapsing. From ENISA's vantage point, what does that episode reveal about the structural fragility of a vulnerability disclosure ecosystem that underpins global cybersecurity?

The CVE Program has long served as the single global reference point for

Featured news

- DarkMoon: Open-source AI pentesting platform
- Synology issues critical fix for MailPlus Server vulnerabilities
- Mystery hackers use novel SharkLoader dropper against governments, software devs

Resources

- Download: Secure Foundations for AI Workloads on AWS
- Download: Automating Pentest Delivery Guide
- CIS Benchmarks March 2026 Update

Apr 15, 2026 · ONLINE

Interview

Coordinated vulnerability disclosure is now an...

helpnetsecurity.com/2026/04/15/nuno-ro...

Estimated Views

1.29K

Engagements

13



Infosecurity Magazine

The award winning online magazine dedicated to the strategy, insight and technology of information...

71

Domain Authority [?]

Provided by
MOZ

109K

Unique Visits [?]

Provided by
SimilarWeb

Apr 15, 2026 · ONLINE

News

ENISA Seeks Top-Tier Status in CVE Program

infosecurity-magazine.com/news/enisa-e...

Estimated Views

833

Engagements

8

Infosecurity Magazine

Log InSign Up

NewsTopicsFeaturesWebinarsWhite PapersPodcastsEventsDirectory

Infosecurity Magazine Home » News » European Cybersecurity Agency ENISA Seeks Top-Tier Status in CVE Program

NEWS15 April 2026

European Cybersecurity Agency ENISA Seeks Top-Tier Status in CVE Program

Kevin Poireault
Reporter, Infosecurity Magazine
Follow @KpoireaultConnect on LinkedIn

ENISA, the EU's Cybersecurity Agency, is strengthening its ties with the US-funded Common Vulnerabilities and Exposures (CVE) program, a top leader of the agency has announced.

Invited to speak at VulnCon26's opening keynote in Scottsdale, Arizona, on April 14, Nuno Rodrigues Carvalho, head of sector for Incidents and Vulnerability Services at ENISA, revealed that the agency was currently being onboarded by the US Cybersecurity and Infrastructure Security Agency (CISA), sole sponsor of the program, to become a top-level root CVE Numbering Authority (TL-Root CNA).

Speaking to *Infosecurity* after the session, Carvalho said he hopes the European agency can obtain this status "in 2026 or early 2027."

CNA. Root CNA and TL-

You may also like

NEWS15 April 2026

AI Companies to Play Bigger Role in CVE Program, Says CISA

NEWS3 July 2025

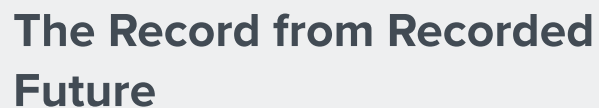
CVE Program Launches Two New Forums to Enhance CVE Utilization

NEWS17 April 2025

CISA Throws Lifeline to CVE Program with Last-Minute Contract Extension

NEWS23 May 2024

NVD Leaves Exploited Vulnerabilities Unchecked



65
Domain
Authority 
Provided by
MOZ

Apr 16, 2026 ·  ONLINE

NIST to limit work on CVE entries as submissions surge

[therecord.media/nist-to-limit-work-on-cve...](https://therecord.media/nist-to-limit-work-on-cve-2022-0788/)

Estimated Views

2.02K

Engagements

193



NIST to limit work on CVE entries as submissions surge

Starting on Wednesday, NIST will only enrich CVEs that appear in a **federal catalog** of exploited vulnerabilities organized by the Cybersecurity and Infrastructure Security Agency

First stalkerware maker prosecuted since 2014 receives no jail time | April 6th, 2026

CSO

CSO Online

CSO delivers the critical information about trends, practices, and products enterprise security leaders...

84

Domain
Authority [?]

Provided by
MOZ

165K

Unique
Visits [?]

Provided by
SimilarWeb

Apr 17, 2026 ·  ONLINE

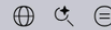
NIST cuts down CVE analysis amid vulnerability overload

csoonline.com/article/4159882/nist-cuts-d...

Estimated Views

671

Engagements

2**CSO**

Home • Security • Vulnerabilities



by **Maria Korolov**
Contributing writer



Updated

NIST cuts down CVE analysis amid vulnerability overload

News

Apr 16, 2026 • 5 mins

The agency will only add enrichment details to CVEs in limited cases going forward, prioritizing known exploited flaws and vaguely defined 'critical software.'



Credit: Elnur / Shutterstock

Overwhelmed by an escalating volume of security flaws, the National Institute of Standards and Technology (NIST) has announced significant changes to how it handles cybersecurity vulnerabilities and exposures (CVEs).

Rather than commit to providing enrichment for all entries

cyberdefensewire.com

25
Domain
Authority ⓘ
Provided by
MOZ

2.56K
Unique
Visits ⓘ
Provided by
SimilarWeb

🌐 ONLINE

FIRST Wraps CVE/VulnCon 2026 with 500+ Attendee...

[cyberdefensewire.com/first-wraps-cve-vuln...](https://cyberdefensewire.com/first-wraps-cve-vulncon-2026-with-500-plus-attendees/)

Estimated Views

1.11K



Le Monde Informatique : actualités, dossiers et tendances IT

Retrouvez l'actualité, les dossiers, les chroniques et les tendances IT au service des métiers et des...

65

Domain Authority ?

Provided by MOZ

139K

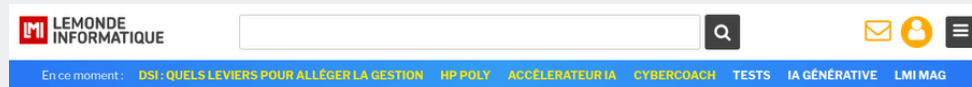
Unique Visits ?

Provided by SimilarWeb

Apr 17, 2026 · ONLINE

Submergé par les failles, le NIST se concentre sur les pl...

lemondeinformatique.fr/actualites/lire-sub...

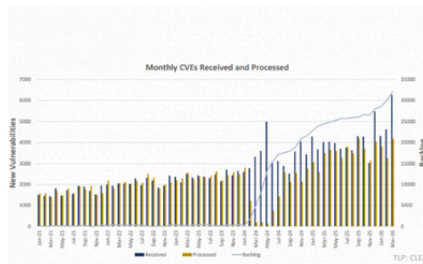


TOUTE L'ACTUALITÉ / SÉCURITÉ

Submergé par les failles, le NIST se concentre sur les plus critiques

Maria Korolov, CSO (adapté par Dominique Filippone), publié le 17 Avril 2026

Suite à un afflux de failles à traiter, l'Institut national des normes et des technologies compte désormais donner la priorité à celles dont l'exploitation est avérée ou affectant des logiciels considérés comme critiques.



Evolution mensuelle du nombre de CVE reçues et traitées par le NIST. (crédit : NIST)

Assailli par un nombre croissant de failles de sécurité à traiter, l'Institut national des normes et des technologies (NIST) a annoncé des changements importants dans la manière dont il traite les vulnérabilités et les expositions en matière de cybersécurité (CVE). Plutôt que de s'engager à enrichir toutes les entrées de sa base de données nationale sur les vulnérabilités (NVD), l'agence se

SUIVRE TOUTE L'ACTUALITÉ

Newsletter

Recevez notre newsletter comme plus de 50 000 professionnels de l'IT!

JE M'ABONNE

Estimated Views

1.08K



Infosecurity Magazine

The award winning online magazine dedicated to the strategy, insight and technology of information...

71

Domain Authority [?]

Provided by
MOZ

109K

Unique Visits [?]

Provided by
SimilarWeb

The screenshot shows the Infosecurity Magazine website. The header includes the logo, navigation links (News, Topics, Features, Webinars, White Papers, Podcasts, Events, Directory), and a search icon. The main article is titled "FIRST CEO Calls for Global CVE Collaboration amid AI Vulnerability Tsunami" by Kevin Poireault, dated 17 April 2026. The article text discusses the rapidly evolving software vulnerability landscape and the need for global cooperation. A "You may also like" section on the right lists related articles, including "#Infosec2025: How Security Teams Can Make Sense of the Vulnerability Conundrum (video)" and "Infosecurity Europe: Patch Responsibility Remains Up for Grabs as AI Unearths Decades of Flaws".

Apr 17, 2026 · ONLINE

Interview

FIRST CEO Calls for CVE Collaboration amid AI Vulnerabilit...

infosecurity-magazine.com/interviews/firs...

Estimated Views

826

Engagements

4



Security Point Break

Security Point Break: Cybersecurity news and analysis with clarity, candor, and human intelligence.

7
Domain
Authority ?
Provided by
MOZ

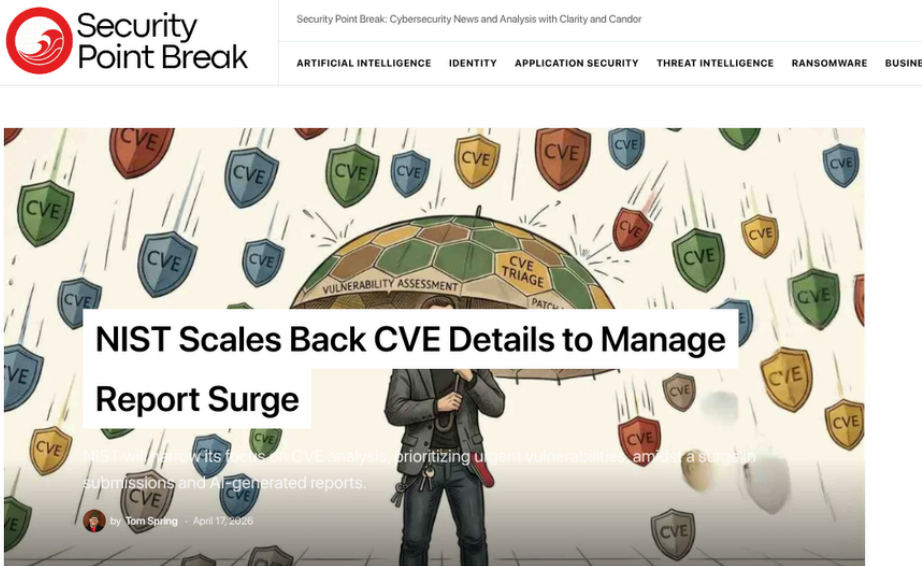
25
Unique
Visits ?
Provided by
SimilarWeb

Apr 17, 2026 · ONLINE News

NIST Scales Back CVE Details to Manage Report Surge NIST...

securitypointbreak.com/2026/04/17/nist-s...

Estimated Views 11
Engagements 1



f A surge in vulnerability submissions is forcing the National Institute of Standards and Technology, the U.S. agency that helps maintain the National Vulnerability Database, to narrow how it handles Common Vulnerabilities and Exposures, or CVEs. Starting April 15, 2026, NIST said it will focus its added analysis on a smaller set of the most urgent flaws.

X That added analysis, often called enrichment, gives security teams valuable information to prioritize patches. NIST has traditionally added items such as severity scores and affected product lists to all CVE records.

@ NIST said CVE submissions rose 263% between 2020 and 2025. "We are working faster than ever. We enriched nearly 42,000 CVEs in 2025 — 45% more than any prior year," NIST wrote.

Cybersecurity professionals have reacted with a mix of concern and understanding. The move is risky because it removes context many teams use for triage. It will also force defenders to rely more on vendor advisories, CISA, CNAs and commercial tools rather than treat the NVD as a one-stop prioritization source, according to comments published by ITPro.

Now NIST will concentrate that work on three groups: vulnerabilities in CISA's Known Exploited Vulnerabilities catalog, software used by the federal government and "critical software" covered by Executive Order 14028. NIST said it aims to enrich KEV-listed flaws within one business day of receipt.



Dark Reading

Dark Reading: Connecting The Cybersecurity Community.

82

Domain Authority ?

Provided by
MOZ

194K

Unique Visits ?

Provided by
SimilarWeb

SearchSecurityCybersecurity DiveInformationWeekChannel DiveExplore our brands

Dark Reading Resource LibraryBlack Hat NewsOmdia CybersecurityAdvertise

20th ANNIVERSARY

DARK READING

NEWSLETTER SIGN-UP

Cybersecurity TopicsWorldThe EdgeDR TechnologyEventsResources

THREAT INTELLIGENCEVULNERABILITIES & THREATSCYBERATTACKS & DATA BREACHESNEWS

How NIST's Cutback of CVE Handling Impacts Cyber Teams

Industry and ad hoc coalitions appear poised to help fill the gap created by NIST's decision to cut back on CVE data enrichment.



Becky Bracken, Senior Editor, Dark Reading
April 17, 2026

7 Min Read

Editor's Choice



SOURCE: GRANDBROTHERS VIA ALAMY STOCK PHOTO

in

f

X

reddit

twitter

email

The chilly air-conditioned Scottsdale ballroom hardly stirred while Harold Booth, program manager for NIST's National Vulnerability Database (NVD), discussed a major operational change — his organization is scaling back its operations and will prioritize which CVEs are chosen for enrichment rather than taking them all on

CYBERSECURITY OPERATIONS

DARK READING CONFIDENTIAL

Do CISOs Need a Code of Ethics?

by Dark Reading Editorial Team

JUN 24, 2026

CYBERSECURITY OPERATIONS



2026 FIFA World Cup Faces Surge in Cyber Threats

by Alexander Culafi

JUN 24, 20263 MIN READ

Apr 17, 2026 · ONLINE

News

How NIST's Cutback of CVE Handling Impacts Cyber Teams

darkreading.com/threat-intelligence/nist-...

Estimated Views

933

FIRST Q2FY26 PR Coverage (As of 6.29.26)

26



ChannelLife US

ChannelLife US is a live news website with regular email newsletters dedicated to the US's technolog...

23

Domain
Authority ?

Provided by
MOZ

2.67K

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

channellife.news/story/first-conference-hi...

Estimated Views

1.23K

Engagements

1

ChannelLife US - Industry insider news for technology resellers

ChannelLife UNITED STATES

POWERED BY TechDay

GUIDES | Cloud Services | Cybersecurity | Distributors | Microsoft | Partner Programmes

Search...



IOT SECURITY | APPLICATION SECURITY | SUPPLY CHAIN

FIRST conference highlights AI & CVE disclosure push

Fri, 17th Apr 2026

Related stories

- Akto widens AI agent security with new integrations
- Red Hat survey finds cloud security incidents rife
- AI-driven cyber wars to reshape security in 2026
- IBM & Red Hat launch £5bn open-source security plan
- KnowBe4 partners Secure Code Warrior on AI training

Top stories

- OWC launches Atlas Core CFexpress 4.0 card for creators
- Cisco and OpenAI outline AI's growing role in cyber defence
- Microsoft launches Copilot AI defense capabilities

JOSEPH GABRIEL LAGONSIN
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



ChannelLife Canada

ChannelLife Canada is a live news website with regular email newsletters dedicated to Canada's...

24

Domain
Authority ?

Provided by
MOZ

1.71K

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

channellife.ca/story/first-conference-highl...

Estimated Views

758

ChannelLife Canada - Industry insider news for technology resellers

ChannelLife

CANADA

POWERED BY

TechDay

GUIDES

Cloud Services

Cybersecurity

Distributors

Microsoft

Partner Programmes



FIRST conference highlights AI & CVE disclosure push

Fri, 17th Apr 2026

Related stories

Red Hat survey finds cloud security incidents rife

AI-driven cyber wars to reshape security in 2026

IBM & Red Hat launch £5bn open-source security plan

KnowBe4 partners Secure Code Warrior on AI training

Orca Security flags AI secrets & supply chain gaps

Top stories

Cisco and OpenAI outline AI's growing role in cyber defence

Wise Up PR wins SPARC AI defence communications brief

Week 1: top 100 CISOs test cloud solutions



JOSEPH GABRIEL LAGONSIN
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



ChannelLife Ireland

ChannelLife Ireland is a live news website with regular email newsletters dedicated to Ireland's technology channel, in particular...

15

Domain
Authority [?]

Provided by
MOZ

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

channellife.ie/story/first-conference-highli...

ChannelLife Ireland - Industry insider news for technology resellers

POWERED BY

GUIDES

Cloud Services Cybersecurity Distributors Microsoft Partner Programmes

Search...

FIRST conference highlights AI & CVE disclosure push

Fri, 17th Apr 2026

Related stories

- Red Hat survey finds cloud security incidents rife
- IBM & Red Hat launch £5bn open-source security plan
- KnowBe4 partners Secure Code Warrior on AI training
- Cloudsmith survey finds SBOM gaps before cyber law
- Orca Security flags AI secrets & supply chain gaps

Top stories

- Cisco and OpenAI outline AI's growing role in cyber defence
- Wise Up PR wins SPARC AI defence communications brief
- OpenAI and Google launch AI safety framework



JOSEPH GABRIEL LAGONSIN
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



ChannelLife UK

ChannelLife UK is a live news website with regular email newsletters dedicated to the United...

35

Domain
Authority ?

Provided by
MOZ

3.64K

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

channellife.co.uk/story/first-conference-hi...

Estimated Views

943

ChannelLife UK - Industry insider news for technology resellers

ChannelLife
UNITED KINGDOM

POWERED BY
TechDay

[GUIDES](#) | [Cloud Services](#) | [Cybersecurity](#) | [Distributors](#) | [Microsoft](#) | [Partner Programmes](#) |



[IOT SECURITY](#) | [APPLICATION SECURITY](#) | [SUPPLY CHAIN](#)

FIRST conference highlights AI & CVE disclosure push

Fri, 17th Apr 2026

Related stories

- Red Hat survey finds cloud security incidents rife
- IBM & Red Hat launch £5bn open-source security plan
- KnowBe4 partners Secure Code Warrior on AI training
- Anthropic AI's Mythos triggers warnings over cyber risk
- Cloudsmith survey finds SBOM gaps before cyber law

**JOSEPH GABRIEL LAGONSIN**
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.

Top stories

- Cisco and OpenAI outline AI's growing role in cyber defence
- Wise Up PR wins SPARC AI defence communications brief
- Compassion and Security for Self-Defence



IT Brief Canada

Dedicated to IT decision-makers at enterprise, corporate, and government organisations...

26

Domain
Authority ?

Provided by
MOZ

4.89K

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

itbrief.ca/story/first-conference-highlights-...

Estimated Views

2.04K

IT Brief Canada - Technology news for CIOs & IT decision-makers

ITBrief
CANADA

POWERED BY
TechDay

GUIDES

Artificial Intelligence

Digital Transformation

Disaster Recovery

Hybrid & Remote Work

Internet of Things

Search...



IOT SECURITY

APPLICATION SECURITY

SUPPLY CHAIN

FIRST conference highlights AI & CVE disclosure push

Fri, 17th Apr 2026

Related stories

Humanoid robots, 0-day defence among Info-Tech trends for '27

Capsule Security raises \$7 million to guard AI agents

Insight launches managed defence for AI-driven flaws

IBM & Red Hat launch £5bn open-source security plan

KnowBe4 partners Secure Code Warrior on AI training

**JOSEPH GABRIEL LAGONSIN**
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.

Top stories

Cisco and OpenAI outline AI's growing role in cyber defence

Wise Up PR wins SPARC AI defence communications brief

FIRST Q2FY26 PR Coverage (As of 6.29.26)

31



IT Brief Ireland

Dedicated to IT decision-makers at enterprise, corporate, and government organisations...

15

Domain Authority ?

Provided by
MOZ

439

Unique Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

itbrief.ie/story/first-conference-highlights-...

Estimated Views

264

IT Brief Ireland - Technology news for CIOs & IT decision-makers

ITBrief
IRELAND

POWERED BY
TechDay

GUIDES

Artificial Intelligence

Digital Transformation

Disaster Recovery

Hybrid & Remote Work

Internet of Things

Search...



IOT SECURITY

APPLICATION SECURITY

SUPPLY CHAIN

FIRST conference highlights AI & CVE disclosure push

Fri, 17th Apr 2026

Related stories

Humanoid robots, 0-day defence among Info-Tech trends for '27

Chief information security officers face pressure over flaws

Insight launches managed defence for AI-driven flaws

IBM & Red Hat launch £5bn open-source security plan

KnowBe4 partners Secure Code Warrior on AI training

Top stories

Wise Up PR wins SPARC AI defence communications brief

Coma earns second Gartner nod for SaaS management

**JOSEPH GABRIEL LAGONSIN**
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.

FIRST Q2FY26 PR Coverage (As of 6.29.26)

32



IT Brief UK

Dedicated to IT decision-makers at enterprise, corporate, and government organisations...

37

Domain Authority ?

Provided by
MOZ

21K

Unique Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

itbrief.co.uk/story/first-conference-highlig...

Estimated Views

4.42K

IT Brief UK - Technology news for CIOs & IT decision-makers

UNITED KINGDOM

POWERED BY

GUIDES | Artificial Intelligence | Digital Transformation | Disaster Recovery | Hybrid & Remote Work | Internet of Things

Search... Q

FIRST conference highlights AI & CVE disclosure push

Fri, 17th Apr 2026

IOT SECURITY **APPLICATION SECURITY** **SUPPLY CHAIN**

Related stories

Humanoid robots, 0-day defence among Info-Tech trends for '27

Chief information security officers face pressure over flaws

Insight launches managed defence for AI-driven flaws

IBM & Red Hat launch £5bn open-source security plan

KnowBe4 partners Secure Code Warrior on AI training

Top stories

Ransomware hits European suppliers as attacks surge 55%

Cisco and OpenAI outline AI's growing role in cyber defence

JOSEPH GABRIEL LAGONSIN
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



IT Brief US

Dedicated to IT decision-makers at enterprise, corporate, and government organisations...

35

Domain
Authority ?

Provided by
MOZ

6.29K

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

itbrief.news/story/first-conference-highlig...

Estimated Views

1.62K

IT Brief US - Technology news for CIOs & IT decision-makers

ITBrief UNITED STATES

POWERED BY **TechDay**

GUIDES | Artificial Intelligence | Digital Transformation | Disaster Recovery | Hybrid & Remote Work | Internet of Things | Search...

FIRST conference highlights AI & CVE disclosure push

Fri, 17th Apr 2026

Related stories

- Humanoid robots, 0-day defence among Info-Tech trends for '27
- Akto widens AI agent security with new integrations
- Insight launches managed defence for AI-driven flaws
- IBM & Red Hat launch £5bn open-source security plan
- KnowBe4 partners Secure Code Warrior on AI training

Top stories

- Cisco and OpenAI outline AI's growing role in cyber defence
- Ondo launches 24/7 minting for tokenised US stocks
- Microsoft and OpenAI address AI defence capabilities

JOSEPH GABRIEL LAGONSIN
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



SecurityBrief Canada

SecurityBrief Canada is focused on cybersecurity and cyberattack news. Its readers include business...

22

Domain
Authority ?

Provided by
MOZ

1.64K

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

securitybrief.ca/story/first-conference-hig...

Estimated Views

770

SecurityBrief Canada - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief
CANADA

POWERED BY
TechDay

GUIDES

Cloud Security

Cybersecurity

Endpoint Protection

Firewalls

Ransomware

Search...



IOT SECURITY

APPLICATION SECURITY

SUPPLY CHAIN

FIRST conference highlights AI & CVE disclosure push

Fri, 17th Apr 2026

Related stories

Humanoid robots, 0-day defence among Info-Tech trends for '27

Capsule Security raises \$7 million to guard AI agents

Anthropic launches Glasswing AI cyber coalition with partners

Red Hat survey finds cloud security incidents rife

Red Hat finds cloud security incidents hit 97% of firms

Top stories

Cisco and OpenAI outline AI's growing role in cyber defence

PDQ launches AI-assisted package builder for IT teams

**JOSEPH GABRIEL LAGONSIN**
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.

FIRST Q2FY26 PR Coverage (As of 6.29.26)

35



SecurityBrief Ireland

SecurityBrief Ireland is focused on cybersecurity and cyberattack news. Its readers include business...

17

Domain Authority ?

Provided by
MOZ

348

Unique Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

securitybrief.ie/story/first-conference-high...

Estimated Views

195

SecurityBrief Ireland - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief

IRELAND

POWERED BY

TechDay

GUIDES

Cloud Security

Cybersecurity

Endpoint Protection

Firewalls

Ransomware

Search...



IOT SECURITY

APPLICATION SECURITY

SUPPLY CHAIN

FIRST conference highlights AI & CVE disclosure push

Fri, 17th Apr 2026

Related stories

Humanoid robots, 0-day defence among Info-Tech trends for '27

Capsule Security raises \$7 million to guard AI agents

Anthropic launches Glasswing AI cyber coalition with partners

Red Hat survey finds cloud security incidents rife

Red Hat finds cloud security incidents hit 97% of firms

Top stories

Ransomware hits European suppliers as attacks surge 55%

Cisco and OpenAI outline AI's growing role in cyber defence

**JOSEPH GABRIEL LAGONSIN**
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.

FIRST Q2FY26 PR Coverage (As of 6.29.26)

36



SecurityBrief India

SecurityBrief India is focused on cybersecurity and cyberattack news. Its readers include business an...

24

Domain
Authority ?

Provided by
MOZ

1.97K

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

securitybrief.in/story/first-conference-high...

Estimated Views

866

SecurityBrief India - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief INDIA

POWERED BY **TechDay**

GUIDES | Cloud Security | Cybersecurity | Endpoint Protection | Firewalls | Ransomware | Search...



FIRST conference highlights AI & CVE disclosure push

Sat, 18th Apr 2026

Related stories

- Capsule Security raises \$7 million to guard AI agents
- Anthropic launches Glasswing AI cyber coalition with partners
- JFrog & iZeno expand AI security tools in Southeast Asia
- Red Hat survey finds cloud security incidents rife
- Red Hat finds cloud security incidents hit 97% of firms

Top stories

- Cisco and OpenAI outline AI's growing role in cyber defence
- PDQ launches AI-assisted package builder for IT teams
- Global Cybersecurity Skills Gap Report

JOSEPH GABRIEL LAGONSIN
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



SecurityBrief US

SecurityBrief US is focused on cybersecurity and cyberattack news. Its readers include business an...

29

Domain
Authority ?

Provided by
MOZ

214

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

securitybrief.news/story/first-conference-...

Estimated Views

65

SecurityBrief US - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief
UNITED STATES

POWERED BY
TechDay

GUIDES

Cloud Security

Cybersecurity

Endpoint Protection

Firewalls

Ransomware

Search...



IOT SECURITY

APPLICATION SECURITY

SUPPLY CHAIN

FIRST conference highlights AI & CVE disclosure push

Fri, 17th Apr 2026

Related stories

Humanoid robots, 0-day defence among Info-Tech trends for '27

Akto widens AI agent security with new integrations

Capsule Security raises \$7 million to guard AI agents

Anthropic launches Glasswing AI cyber coalition with partners

Red Hat survey finds cloud security incidents rife

 **JOSEPH GABRIEL LAGONSIN**
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.

Top stories

Cisco and OpenAI outline AI's growing role in cyber defence

PDQ launches AI-assisted package builder for IT teams



SecurityBrief UK

SecurityBrief UK is focused on cybersecurity and cyberattack news. Its readers include business an...

42

Domain
Authority ?

Provided by
MOZ

9.5K

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

securitybrief.co.uk/story/first-conference-...

Estimated Views

1.28K

SecurityBrief UK - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief
UNITED KINGDOM

POWERED BY
TechDay

GUIDES

Cloud Security

Cybersecurity

Endpoint Protection

Firewalls

Ransomware

Search...



IOT SECURITY

APPLICATION SECURITY

SUPPLY CHAIN

FIRST conference highlights AI & CVE disclosure push

Fri, 17th Apr 2026

Related stories

Humanoid robots, 0-day defence among Info-Tech trends for '27

Capsule Security raises \$7 million to guard AI agents

Anthropic launches Glasswing AI cyber coalition with partners

Red Hat survey finds cloud security incidents rife

Red Hat finds cloud security incidents hit 97% of firms

Top stories

Coma earns second Gartner nod for SaaS management

UK fraud losses hit GBP £1.28 billion as scams rise

UK cyber security spending to rise to £1.2bn in 2026

**JOSEPH GABRIEL LAGONSIN**
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.

FIRST Q2FY26 PR Coverage (As of 6.29.26)

39



ChannelLife Australia

ChannelLife Australia is a live news website with regular email newsletters dedicated to Australia's...

46

Domain Authority ?

Provided by
MOZ

12.5K

Unique Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

channellife.com.au/story/first-conference-...

Estimated Views

1.25K

ChannelLife Australia - Industry insider news for technology resellers

POWERED BY
TechDay

GUIDES

Cloud Services Cybersecurity Distributors Microsoft Partner Programmes

Search... Q

FIRST conference highlights AI & CVE disclosure push

Sat, 18th Apr 2026

IOT SECURITY APPLICATION SECURITY SUPPLY CHAIN

Related stories

Red Hat survey finds cloud security incidents rife

Why organisations in Asia Pacific are rethinking their AI deployment strategies

IBM & Red Hat launch £5bn open-source security plan

KnowBe4 partners Secure Code Warrior on AI training

Melbourne to host combined cyber security conferences

Top stories

Cisco and OpenAI outline AI's growing role in cyber defence

Wise Up PR wins SPARC AI defence communications brief

JOSEPH GABRIEL LAGONSIN
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



ChannelLife India

ChannelLife India is a live news website with regular email newsletters dedicated to India's technology...

24

Domain
Authority ?

Provided by
MOZ

2.22K

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

channellife.in/story/first-conference-highli...

Estimated Views

1.03K

ChannelLife India - Industry insider news for technology resellers

ChannelLife
INDIA

POWERED BY
TechDay

[GUIDES](#) | [Cloud Services](#) | [Cybersecurity](#) | [Distributors](#) | [Microsoft](#) | [Partner Programmes](#) |



[IOT SECURITY](#) | [APPLICATION SECURITY](#) | [SUPPLY CHAIN](#)

FIRST conference highlights AI & CVE disclosure push

Sat, 18th Apr 2026

Related stories

- Red Hat survey finds cloud security incidents rife
- AI-driven cyber wars to reshape security in 2026
- Why organisations in Asia Pacific are rethinking their AI deployment strategies
- IBM & Red Hat launch £5bn open-source security plan
- KnowBe4 partners Secure Code Warrior on AI training

**JOSEPH GABRIEL LAGONSIN**
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.

Top stories

- Cisco and OpenAI outline AI's growing role in cyber defence
- Wise Up PR wins SPARC AI defence communications brief



ChannelLife New Zealand

ChannelLife NZ is a live news website with regular email newsletters dedicated to New Zealand's...

42

Domain
Authority ?

Provided by
MOZ

3.93K

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

channellife.co.nz/story/first-conference-hi...

Estimated Views

589

ChannelLife New Zealand - Industry insider news for technology resellers

ChannelLife
NEW ZEALAND

POWERED BY
TechDay

[GUIDES](#) | [Cloud Services](#) | [Cybersecurity](#) | [Distributors](#) | [Microsoft](#) | [Partner Programmes](#) |



[IOT SECURITY](#) | [APPLICATION SECURITY](#) | [SUPPLY CHAIN](#)

FIRST conference highlights AI & CVE disclosure push

Sat, 18th Apr 2026

Related stories

- Red Hat survey finds cloud security incidents rife
- Why organisations in Asia Pacific are rethinking their AI deployment strategies
- IBM & Red Hat launch £5bn open-source security plan
- KnowBe4 partners Secure Code Warrior on AI training
- Orca Security flags AI secrets & supply chain gaps



JOSEPH GABRIEL LAGONSIN
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.

Top stories

- Wise Up PR wins SPARC AI defence communications brief
- Wasabi launches Impact Circle to track cloud emissions
- Microsoft's National Cyber Security Centre for AI



IT Brief Asia

Dedicated to IT decision-makers at enterprise, corporate, and government organisations...

37

Domain Authority ?

Provided by
MOZ

15.7K

Unique Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

itbrief.asia/story/first-conference-highlight...

Estimated Views

3.61K

IT Brief Asia - Technology news for CIOs & IT decision-makers

POWERED BY
TechDay

GUIDES | Artificial Intelligence | Digital Transformation | Disaster Recovery | Hybrid & Remote Work | Internet of Things

Search...

IOT SECURITY **APPLICATION SECURITY** **SUPPLY CHAIN**

FIRST conference highlights AI & CVE disclosure push

Sat, 18th Apr 2026

Related stories

- Singapore software security gap exposed in JFrog study
- Why organisations in Asia Pacific are rethinking their AI deployment strategies
- Insight launches managed defence for AI-driven flaws
- IBM & Red Hat launch £5bn open-source security plan
- KnowBe4 partners Secure Code Warrior on AI training

Top stories

- Cisco and OpenAI outline AI's growing role in cyber defence
- Wise Up PR wins SPARC AI defence communications brief

JOSEPH GABRIEL LAGONSIN
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



IT Brief Australia

IT Brief is a live news website and weekly email newsletter dedicated to IT Managers & CIO's at...

48

Domain
Authority ?

Provided by
MOZ

26.6K

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

itbrief.com.au/story/first-conference-highli...

Estimated Views

1.24K

IT Brief Australia - Technology news for CIOs & IT decision-makers

ITBrief
AUSTRALIA

POWERED BY
TechDay

GUIDES

Artificial Intelligence

Digital Transformation

Disaster Recovery

Hybrid & Remote Work

Internet of Things

Search...



IOT SECURITY

APPLICATION SECURITY

SUPPLY CHAIN

FIRST conference highlights AI & CVE disclosure push

Sat, 18th Apr 2026

Related stories

Why organisations in Asia Pacific are rethinking their AI deployment strategies

Insight launches managed defence for AI-driven flaws

IBM & Red Hat launch £5bn open-source security plan

KnowBe4 partners Secure Code Warrior on AI training

Cloudflare warns of AI code review prompt injection

Top stories

Cisco and OpenAI outline AI's growing role in cyber defence

Wise Up PR wins SPARC AI defence communications brief

**JOSEPH GABRIEL LAGONSIN**
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



IT Brief India

IT Brief is a live news website and weekly email newsletter dedicated to IT Managers & CIO's at...

24

Domain
Authority ?

Provided by
MOZ

3.09K

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

itbrief.in/story/first-conference-highlights-...

Estimated Views

1.35K

IT Brief India - Technology news for CIOs & IT decision-makers

GUIDES

Artificial Intelligence Digital Transformation Disaster Recovery Hybrid & Remote Work Internet of Things

Search...

IOT SECURITY APPLICATION SECURITY SUPPLY CHAIN

FIRST conference highlights AI & CVE disclosure push

Sat, 18th Apr 2026

Related stories

Capsule Security raises \$7 million to guard AI agents

Why organisations in Asia Pacific are rethinking their AI deployment strategies

Insight launches managed defence for AI-driven flaws

IBM & Red Hat launch £5bn open-source security plan

KnowBe4 partners Secure Code Warrior on AI training

Top stories

Cisco and OpenAI outline AI's growing role in cyber defence

Wise Up PR wins SPARC AI defence communications brief

JOSEPH GABRIEL LAGONSIN
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



IT Brief New Zealand

Dedicated to IT decision-makers at enterprise, corporate, and government organisations...

45

Domain Authority ?

Provided by
MOZ

9.71K

Unique Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

itbrief.co.nz/story/first-conference-highlig...

Estimated Views

896

IT Brief New Zealand - Technology news for CIOs & IT decision-makers



POWERED BY

GUIDES | Artificial Intelligence | Digital Transformation | Disaster Recovery | Hybrid & Remote Work | Internet of Things | Search...



FIRST conference highlights AI & CVE disclosure push

Sat, 18th Apr 2026

IOT SECURITY **APPLICATION SECURITY** **SUPPLY CHAIN**

Related stories

- Why organisations in Asia Pacific are rethinking their AI deployment strategies
- Insight launches managed defence for AI-driven flaws
- IBM & Red Hat launch £5bn open-source security plan
- KnowBe4 partners Secure Code Warrior on AI training
- Cloudflare warns of AI code review prompt injection

Top stories

- Wise Up PR wins SPARC AI defence communications brief
- PDQ launches AI-assisted package builder for IT teams
- Global Cybersecurity Summit highlights AI & CVE disclosure push

JOSEPH GABRIEL LAGONSIN
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



SecurityBrief Asia

SecurityBrief Asia is focused on cybersecurity and cyberattack news. Its readers include business an...

43

Domain
Authority ?

Provided by
MOZ

7.79K

Unique
Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

securitybrief.asia/story/first-conference-hi...

Estimated Views

1.05K

SecurityBrief Asia - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief ASIA

POWERED BY TechDay

GUIDES | Cloud Security | Cybersecurity | Endpoint Protection | Firewalls | Ransomware | Search...



IOT SECURITY | APPLICATION SECURITY | SUPPLY CHAIN

FIRST conference highlights AI & CVE disclosure push

Sat, 18th Apr 2026

Related stories

- Capsule Security raises \$7 million to guard AI agents
- Anthropic launches Glasswing AI cyber coalition with partners
- JFrog & iZeno expand AI security tools in Southeast Asia
- Red Hat survey finds cloud security incidents rife
- Red Hat finds cloud security incidents hit 97% of firms

Top stories

- Cisco and OpenAI outline AI's growing role in cyber defence
- PDQ launches AI-assisted package builder for IT teams
- Global Cybersecurity Summit highlights AI and CVE disclosure push

JOSEPH GABRIEL LAGONSIN
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



SecurityBrief Australia

SecurityBrief Australia is focused on cybersecurity and cyberattack news. Its readers include business...

46

Domain Authority ?

Provided by
MOZ

19.5K

Unique Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

securitybrief.com.au/story/first-conferenc...

Estimated Views

1.52K

SecurityBrief Australia - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief
AUSTRALIA

POWERED BY
TechDay

GUIDES

Cloud Security

Cybersecurity

Endpoint Protection

Firewalls

Ransomware

Search...



IOT SECURITY

APPLICATION SECURITY

SUPPLY CHAIN

FIRST conference highlights AI & CVE disclosure push

Sat, 18th Apr 2026

Related stories

Capsule Security raises \$7 million to guard AI agents

Anthropic launches Glasswing AI cyber coalition with partners

Red Hat survey finds cloud security incidents rise

Red Hat finds cloud security incidents hit 97% of firms

Insight launches managed defence for AI-driven flaws

Top stories

Cisco and OpenAI outline AI's growing role in cyber defence

PDQ launches AI-assisted package builder for IT teams

Global Cybersecurity Index 2025 released

**JOSEPH GABRIEL LAGONSIN**
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



SecurityBrief New Zealand

SecurityBrief New Zealand is focused on cybersecurity and cyberattack news. Its readers...

44

Domain Authority ?

Provided by
MOZ

7.41K

Unique Visits ?

Provided by
SimilarWeb

Apr 18, 2026 · ONLINE

News

FIRST conference highlights AI & CVE disclosure push

securitybrief.co.nz/story/first-conference-...

Estimated Views

879

SecurityBrief New Zealand - Technology news for CISOs & cybersecurity decision-makers

POWERED BY
TechDay

SecurityBrief
NEW ZEALAND

GUIDES | Cloud Security | Cybersecurity | Endpoint Protection | Firewalls | Ransomware | Search...



FIRST conference highlights AI & CVE disclosure push
Sat, 18th Apr 2026

Related stories

- Capsule Security raises \$7 million to guard AI agents
- Anthropic launches Glasswing AI cyber coalition with partners
- Red Hat survey finds cloud security incidents rise
- Red Hat finds cloud security incidents hit 97% of firms
- Insight launches managed defence for AI-driven flaws

Top stories

- Cisco and OpenAI outline AI's growing role in cyber defence
- PDQ launches AI-assisted package builder for IT teams
- Global Cyber Protection Centre and others...

JOSEPH GABRIEL LAGONSIN
News Editor

FIRST has wrapped up CVE/FIRST VulnCon 2026 and the Annual CNA Summit in Scottsdale. The four-day event drew more than 500 attendees from across the vulnerability management and cybersecurity sectors.

Security professionals, researchers and policymakers gathered to discuss vulnerability disclosure, CVE quality, exploit prediction, coordinated disclosure and the security implications of artificial intelligence. Speakers represented organisations including CISA, ENISA, NIST, Google, Microsoft, NVIDIA, Dell and Cisco.

Discussion also focused on the Common Weakness Enumeration framework and its expanding role in vulnerability disclosure. Alec Summers, CVE/CWE Project Lead and Principal Cybersecurity Engineer at MITRE, said organisations increasingly want more detail on the underlying causes of software flaws, not just confirmation that a vulnerability exists.

"What's changed is that CWE is now becoming a more integral part of vulnerability disclosure itself, as the value of transparent root-cause mapping is more widely appreciated. Simply knowing that a vulnerability exists isn't enough; teams need to understand why it exists in order to prioritize, remediate, and prevent recurrence," Summers said.



CYBR.SEC.Media

CYBR.SEC.Media is the ultimate hub for cybersecurity professionals and enthusiasts,...

16

Domain
Authority ?

Provided by
MOZ

1.41K

Unique
Visits ?

Provided by
SimilarWeb

Apr 20, 2026 · ONLINE

News

NIST Declares “Inbox Zero,” Pulls Back on CVE Enrichment. No...

cybrsecmedia.com/nist-declares-inbox-zero...

Estimated Views

868

Engagements

2

**CYBR.SEC.
MEDIA**

TOPICS ARTICLES BLOGS PODCASTS VIDEOS WEBINARS EVENTS COMMUNITY

SIGN IN

Subscribe

ARTICLE — NIST — CVE — VULNERABILITY MANAGEMENT

NIST Declares “Inbox Zero,” Pulls Back On CVE Enrichment. Now Enterprise Security Teams Must Fill The Gap

An analysis of the National Vulnerability Database's shift to risk-based triage and what it actually means for the people patching systems (first of a two-part analysis)

GEORGE V. HULME

April 20, 2026 · 9:12 AM — 5 min read



The National Institute of Standards and Technology (NIST) has effectively conceded that it can no longer analyze every vulnerability flowing into the National Vulnerability Database (NVD).

“NIST declared inbox zero. Over a year behind, the budget never caught up, and now they're saying the quiet part out loud. Federal priority CVEs get enriched, everything else is on us,” says Andrew Storms, a long-time



Silobreaker

Home

53

Domain
Authority ?

Provided by
MOZ

3.47K

Unique
Visits ?

Provided by
SimilarWeb

Apr 21, 2026 · ONLINE

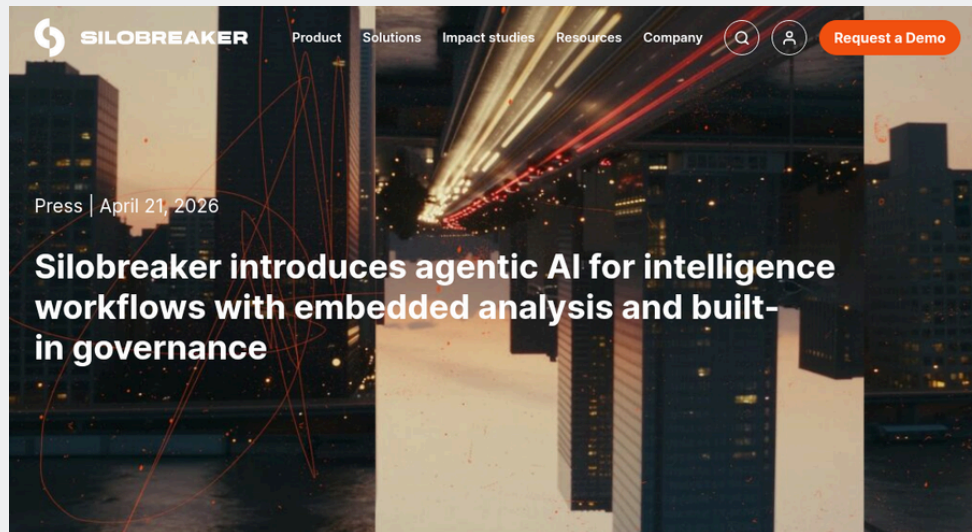
News

Silobreaker introduces agentic AI for intelligence...

silobreaker.com/news/2026/04/silobreak...

Estimated Views

49



Press | April 21, 2026

Silobreaker introduces agentic AI for intelligence workflows with embedded analysis and built-in governance

New capabilities, including Silobreaker Mimir, enable intelligence teams to work faster, and apply richer context, while extending trusted insight across security, risk and enterprise decision-making

SHARE



LONDON – April 21, 2026 – Silobreaker, a leading security and threat intelligence technology company trusted by intelligence consumers, security leaders, risk teams and analysts, today announced new agentic AI capabilities that strengthen its role as a foundational intelligence engine across cyber, geopolitical, physical and operational risk domains. The new capabilities combine faster research and deeper contextual analysis with built-in governance and transparency to ensure trusted intelligence can be safely consumed across the wider enterprise.

Silobreaker Mimir is an embedded agentic capability for intelligence operations, working directly within the analyst workflow. It helps teams retrieve evidence, deepen analysis, and turn validated findings into native assets and stakeholder ready outputs – such as creating dashboards and reports – in a single connected environment. Intelligence teams can scale their coverage of complex evolving stakeholder requirements while maintaining full oversight, with all outputs grounded in verifiable source material and transparent reasoning.

"For intelligence teams, the real challenge is accelerating analysis without losing context, accountability, or trust," said Silobreaker CEO, Geoffrey Brown. "Silobreaker Mimir applies AI



Resilient Cyber | Chris Hughes | Substack

Resilient Cyber distills the week's most important news, research, and writing across AppSec, AI...

30
Domain
Authority 
Provided by
MOZ

3K
Unique
Visits 
Provided by
SimilarWeb

Apr 22, 2026

ONLINE

Comment

The NVD Just Threw In The Towel - Now What?

resilientcyber.io/p/the-nvd-just-threw-in-th...

Resilient Cyber

[Subscribe](#) [Sign in](#)

The NVD Just Threw In The Towel - Now What?

CHRIS HUGHES
APR 22, 2026

14   [Share](#)

A little over a year ago, I wrote [Death Knell of the NVD](#) and even broke down the NVD chaos with Josh Bressers and Dan Lorenc:



The point was, the NIST National Vulnerability Database (NVD) was structurally incapable of keeping pace with the volume and velocity of modern vulnerability disclosures. It was underfunded, understaffed, and operating on a model designed for a world that no longer exists. The backlog was growing, the enrichment pipeline was breaking down, and the industry was placing its trust in a system that could not deliver on the promise of being the authoritative source of vulnerability intelligence.

The NVD was (and still is) dealing with a variety of challenges such as legacy manual processes, contractual hurdles, funding constraints, technical bottlenecks and an ever growing flow of CVE's.

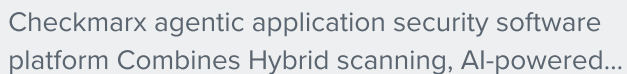
At the time, some people thought I was being dramatic, I was not. NVD's problems have only persisted since then, and now seem to have come to a head.

Estimated Views

1K

Engagements

1



Provided by
MOZ

Provided by
 **SimilarWeb**

Feature

Guardrails for Agentic Development

[checkmarx.com/blog/guardrails-for-agent...](https://checkmarx.com/blog/guardrails-for-agent-frameworks/)

Estimated Views

815

What Effective Governance Looks Like in Practice

The Scale Problem: Vulnerability Growth Is Now an Operational Constraint



Intelligent Application Security Platform | Kodem

The AI-native application security platform powered by runtime intelligence. See which risks actually...

31

Domain Authority 

Provided by
MOZ

2.04K

Unique Visits 

Provided by
SimilarWeb

 ONLINE

Comment

NIST NVD Update: What the 2026 vulnerability...

kodemsecurty.com/resources/nvds-decis...

Estimated Views

769

 Platform Technology Pricing Company Resources Join us Events [Get a demo](#)

[← All Blogs](#) [Copy URL](#) [in](#) [X](#) [f](#)

The NIST NVD update changes vulnerability management more than most teams realize

 Mahesh Babu April 23, 2026 • 7 min read

Vulnerabilities



NIST NVD Update

NIST's [April 15, 2026 update to NVD operations](#) is easy to summarize and easy to underread. The headline change is familiar by now: NIST will continue listing all CVEs, but it will only immediately enrich a subset, prioritizing [CISA KEV](#), software used within the federal government, and software covered by [Executive Order 14028's critical software definition](#). Everything else can land in NVD as "Lowest Priority - not scheduled for immediate enrichment," and NIST will no longer routinely add a second severity score when a CNA already supplied one. NIST says CVE submissions grew 263% from 2020 to 2025, that Q1 2026 volume is nearly as high as ever, and that it enriched nearly 40,000 CVEs in

Table of contents

What actually changed

The non-obvious implication: NVD is ceasing to be the universal translation layer

Why Mythos matters here, even if it is not the headline

This will change what "good" vulnerability management looks like

The uncomfortable part: the ecosystem may become less neutral

What teams should do now

Final thoughts

References



ZAWYA - The trusted source for business and finance news

Latest business, economic and financial markets news, along with insights, research and multimedia

80
Domain
Authority [?]
Provided by
MOZ

254K
Unique
Visits [?]
Provided by
SimilarWeb

Apr 23, 2026 · ONLINE

News

Cybersecurity from Bahrain to the world leading at world lev...

zawya.com/en/press-release/events-and-...

Estimated Views

1.33K

Find news, press releases and more

ZAWYA
BY LSEG

MENA - ENGLISH X f in

CAPITAL MARKETS BUSINESS ECONOMY PROJECTS MULTIMEDIA REPORTS PRESS RELEASE ZAWYA GREEN EVENTS FIND COMPANIES عربي

Special Coverage Abu Dhabi Focus Corporate Earnings UAE Realty Market The Future of Cryptos AI: Shaping Digital Future



CTM360, a Bahrain-based cybersecurity company, showcased its global presence as a Platinum Sponsor at the FIRST Cyber Threat Intelligence (CTI) Conference 2026, held in Munich, Germany. Image courtesy: CTM360

CYBERSECURITY

Cybersecurity from Bahrain to the world leading at world level Cyber Threat Intelligence conference in Germany

At the conference, CTM360 highlighted an intelligence-driven model built on early signals such as Indicators of Exposure, Warning, and Attack, enabling organizations to identify vulnerabilities and act before threats materialize

Press Release

April 23, 2026

Manama, Bahrain – CTM360, a Bahrain-based cybersecurity company, showcased its global presence as a Platinum Sponsor at the FIRST Cyber Threat Intelligence (CTI) Conference 2026, held in Munich, Germany.

The event, organized by the Forum of Incident Response and Security Teams (FIRST), brought

GE f

X

in

RELATED TOPICS

CYBERSECURITY



cyberdefensewire.com

26
Domain
Authority ?
Provided by
MOZ

2.36K
Unique
Visits ?
Provided by
SimilarWeb

🌐 ONLINE

News

FIRST Concludes Sold-Out 2026 Cyber Threat Intelligence...

cyberdefensewire.com/first-concludes-so...

Estimated Views

1K

Call us Toll Free (USA): 1-833-844-9468 International: +1-603-280-4451 M-F 8am to 6pm EST

Cyber Defense Magazine Cyber Defense Awards Cyber Defense Webinars Cyber Defense Conferences Cyber Defense TV Cyber Defense Radio Subscribe

CYBERDEFENSE^{Wire} Home Press Releases Contact [Submit a Press Release](#)

FIRST Concludes Sold-Out 2026 Cyber Threat Intelligence Conference in Munich

in

Global practitioners gathered to advance AI-driven CTI, detection engineering, and threat intelligence standards

MUNICH, GERMANY, APRIL 23, 2026 – Today, the Forum of Incident Response and Security Teams (FIRST) successfully concluded its sold-out **2026 Cyber Threat Intelligence Conference**. The three-day event brought hundreds of professionals from across the cyber threat intelligence landscape together in Munich for workshops, plenary sessions, and hands-on training.

The 2026 program was chaired by Thomas Schreck of Munich University of Applied Sciences and Patrick Grau of Exyte. Sessions were led by practitioners and researchers from Google, AWS, the European Commission CSOC, ENISA, CIRCL (Computer Incident Response Center Luxembourg), CERT-In, Intel 471, Nordic Financial CERT, Sopra Steria, Deloitte, BlackRock, Recruit, CyCraft Technology, Eindhoven University of Technology, NVISO, NTT DATA, Expel, and the Retail & Hospitality ISAC, among others.

"FIRST's Cyber Threat Intelligence Conference gives this community a rare kind of access: direct conversation with the people doing the work, in a format you can't replicate anywhere else," said **Chris Gibson**, CEO, FIRST. "People come here to compare notes on problems they're solving, to meet the researcher(s) whose paper(s) they've been quoting for a year, and to leave with answers they won't find anywhere else. That kind of collaboration has to be built in a room, and that's what this conference is all about."

2026 FIRST Cyber Threat Intelligence Conference

Munich, Germany
April 21-23

Press Release by Forum of Incident Response and Security Teams (FIRST)

Media Contact

Jordan Mitchell
jordan@growthstackmedia.com

Cyber Defense Magazine
June Edition for 2026

[Download eMag](#)

Published monthly by Cyber Defense Magazine, this resource shares a wealth of information to help you stay one step ahead of the next cyber threat.



Vercel Security Checkpoint

VentureBeat is the leader in covering transformative tech. We help business leaders make smarter...

91

Domain
Authority ?

Provided by
MOZ

1.15M

Unique
Visits ?

Provided by
SimilarWeb

Apr 24, 2026 · ONLINE

Feature

CVSS vulnerability triage: 5 failures, 5 fixes

venturebeat.com/security/cvss-triage-fail...

Estimated Views

2.43K

Engagements

7

VB

- Orchestration
- Infrastructure
- Data
- Security
- More ^

Newsletters

Featured

CVSS scored these two Palo Alto CVEs as manageable. Chained, they gave attackers root access to 13,000 devices.

[Louis Columbus](#)

Published

2:34 pm, PT, April 24, 2026

Updated

3:10 pm, PT, April 24, 2026

VentureBeat created with Imagen

During [Operation Lunar Peek in November 2024](#), attackers gained unauthenticated remote admin access — and eventual root — across more than [13,000 exposed Palo Alto Networks management interfaces](#). Palo Alto Networks scored [CVE-2024-0012](#) at 9.3 and [CVE-2024-9474](#) at 6.9 under CVSS v4.0. NVD scored the same pair [9.8 and 7.2 under CVSS v3.1](#). Two scoring systems. Two different answers for the same vulnerabilities. The 6.9 fell below patch thresholds. Admin access appeared required. The 9.3 sat queued for maintenance. Segmentation would hold.

"Adversaries circumvent [severity ratings] by chaining vulnerabilities together," Adam Meyers, SVP of Counter Adversary Operations at CrowdStrike, told VentureBeat in an exclusive interview on April 22, 2026. On the triage logic that missed the chain: "They just had amnesia from 30 seconds before."

Both CVEs sit on the [CISA Known Exploited Vulnerabilities catalog](#). Neither score flagged the kill chain. The triage logic that consumed those scores treated each CVE as an isolated event, and so did the SLA dashboards and the board reports those dashboards feed.

CVSS did exactly what it was designed to do. Score one vulnerability at a time. The problem is that adversaries do not attack one vulnerability at a time.

"CVSS base scores are theoretical measures of severity that ignore real-world context," [wrote](#) Peter Chronis, former CISO of Paramount and a security leader with Fortune 100 experience. By moving beyond CVSS-first prioritization at Paramount, Chronis reported reducing actionable critical and high-risk vulnerabilities by 90%. Chris Gibson, executive director of FIRST, the organization that maintains CVSS, has been equally direct: using CVSS base scores alone for prioritization is "the least apt and accurate" method, Gibson [told The Register](#). FIRST's own [EPSS](#) and CISA's SSVS decision model address part of this gap by adding exploitation probability and decision-tree logic.

Five triage failure classes CVSS was never designed to catch

In 2025, [48,185 CVEs were disclosed](#), a 20.6% year-over-year increase. Jerry Gamblin, principal engineer at Cisco Threat Detection and Response, [projects 70,135 for 2026](#). The infrastructure behind the scores is buckling under that weight. [NIST announced on April 15](#) that CVE submissions have grown 263% since 2020, and the NVD will now prioritize enrichment for KEV and federal critical software only.

1. Chained CVEs that look safe until they aren't

The Palo Alto pair from [Operation Lunar Peek](#) is the textbook. CVE-2024-0012 bypassed authentication. CVE-2024-9474 escalated privileges. Scored separately under both CVSS v4.0 and v3.1, the escalation flaw filtered below most enterprise patch thresholds because admin access appeared required. The authentication bypass upstream eliminated that prerequisite entirely. Neither score communicated the compound effect.

Meyers described the operational psychology: teams assessed each CVE independently, deprioritized the lower score, and queued the higher one for maintenance.

2. [Nation-state adversaries who weaponize patches within days](#)



RocketNews

RocketNews is an news aggregator of the top online news articles and stories from around the globe.

52

Domain
Authority [?]

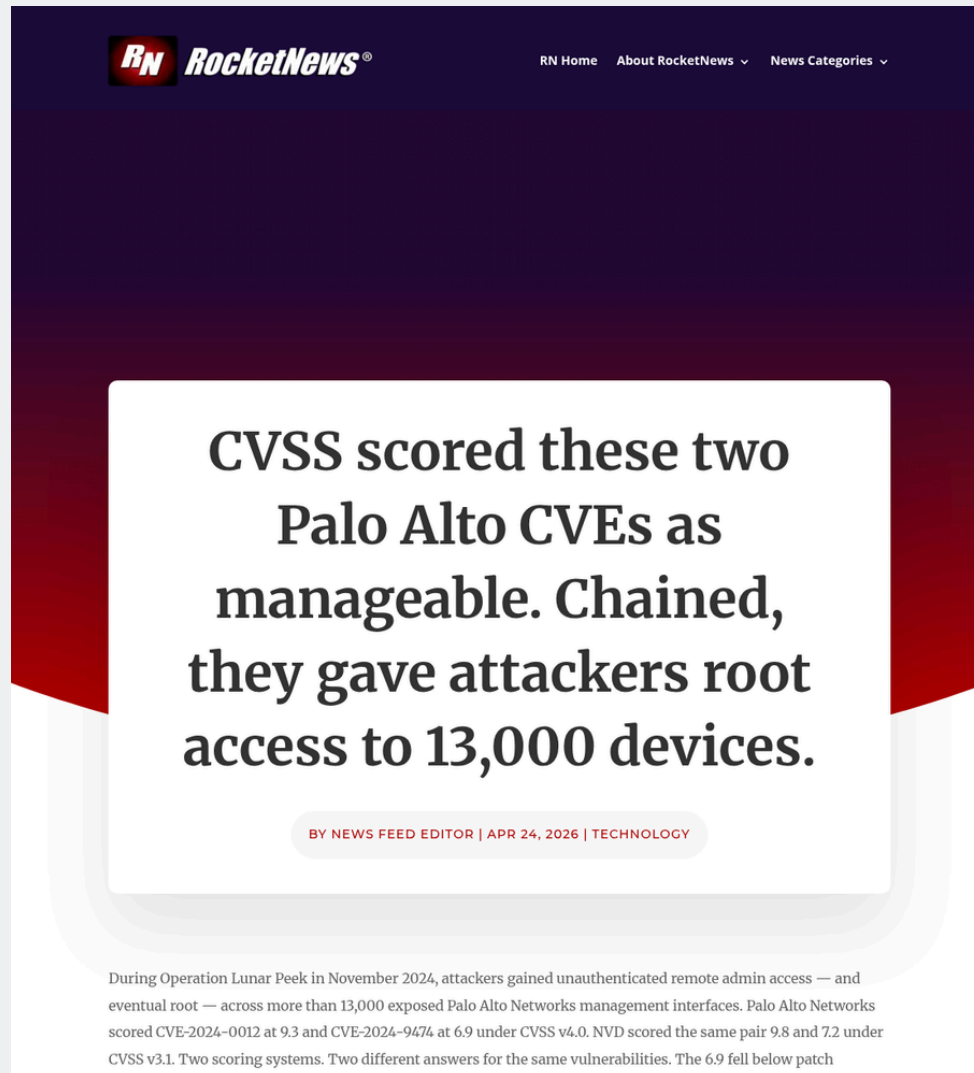
Provided by
MOZ

Apr 24, 2026 ·  ONLINE

News

CVSS scored these two Palo Alto CVEs as manageable....

rocketnews.com/2026/04/cvss-scored-th...





Resilient Cyber | Chris Hughes | Substack

Resilient Cyber distills the week's most important news, research, and writing across AppSec, AI...

30
Domain
Authority 
Provided by
MOZ

3K
Unique
Visits 
Provided by
SimilarWeb

Apr 24, 2026 ·  ONLINE

[Comment](#)

Resilient Cyber Newsletter #94

resilientcyber.io/p/resilient-cyber-newslett...

 **Resilient Cyber**   [Subscribe](#) [Sign in](#)

Resilient Cyber Newsletter #94

Mythos Model Leak, OWASP GenAI Exploit Roundup, OAuth Challenges for Agentic AI, Mythos Delivers 271 Firefox Findings, Vercel Breach & NVD Throws in the Towel

 **CHRIS HUGHES**
APR 24, 2026

 12  2  1 [Share](#)

Welcome to issue #94 of the Resilient Cyber Newsletter!

Last week I wrote that Mythos had crossed from research project to systemic risk. This week, the cracks started showing. Bloomberg reported that an unauthorized group gained access to Mythos through a third-party contractor. The NSA is reportedly using Mythos despite the Pentagon's own supply chain risk designation against Anthropic. OMB clarified that it is not giving agencies access to anything, even as it quietly examines guardrails for a modified version and VulnCheck dug into the actual CVE data behind Project Glasswing and found that only one CVE has been directly tied to the program so far.

At the same time, the defensive ecosystem continued to build.

JPMorgan published a 10-point playbook for AI-ready cyber resilience. Anthropic endorsed EPSS as the triage framework for the coming bug surge, and Empirical Security responded with a sharp piece on why that still leaves the hard part unsolved. Mozilla shipped Firefox 150 with 271 bug fixes discovered by Mythos, roughly four times the annual baseline in a single pass. Semgrep tested whether open source models can replicate what Mythos did and found that discovery is orders of magnitude harder than verification. The Cloud Security Alliance published research showing 53% of organizations report AI agents exceeding intended permissions, and NIST officially stopped enriching most CVEs.

So, yeah, just another light week in cyber, so let's get into it.



RESILIENT CYBER
NEWSLETTER #94
APRIL 23 2026
Mythos Model Leak OWASP GenAI Exploit Roundup

Estimated Views

1K



News Directory 3

Find local newspapers, digital news outlets, news services and current headlines across the United...

48

Domain Authority ?

Provided by MOZ

2.42K

Unique Visits ?

Provided by SimilarWeb

Apr 25, 2026 · ONLINE

Feature

Why CVSS Scores Miss Real-World Threats: Fixing Triag...

newsdirectory3.com/why-cvss-scores-mis...

Estimated Views

75



Why CVSS Scores Miss Real-World Threats: Fixing Triage Failures in the AI Era

April 25, 2026 · Lisa Park · Tech

NEWS CONTEXT

At a glance

- The recent exploitation of two vulnerabilities in Palo Alto Networks systems, which together granted attackers unauthenticated remote admin access and eventual root control over more than 13,000 exposed...
- During Operation Lunar Peek in November 2024, attackers leveraged CVE-2024-0012, scored 9.3 by Palo Alto Networks under CVSS v4.0 (9.8 in NVD's CVSS v3.1), to bypass authentication, and...
- Adam Meyers, SVP of Counter Adversary Operations at CrowdStrike, noted in an exclusive interview with VentureBeat on April 22, 2026, that adversaries circumvent severity ratings by chaining



World Today Journal

World Today Journal delivers breaking world news, business, technology, sports, health and...

40

Domain
Authority ?

Provided by
MOZ

2.14K

Unique
Visits ?

Provided by
SimilarWeb

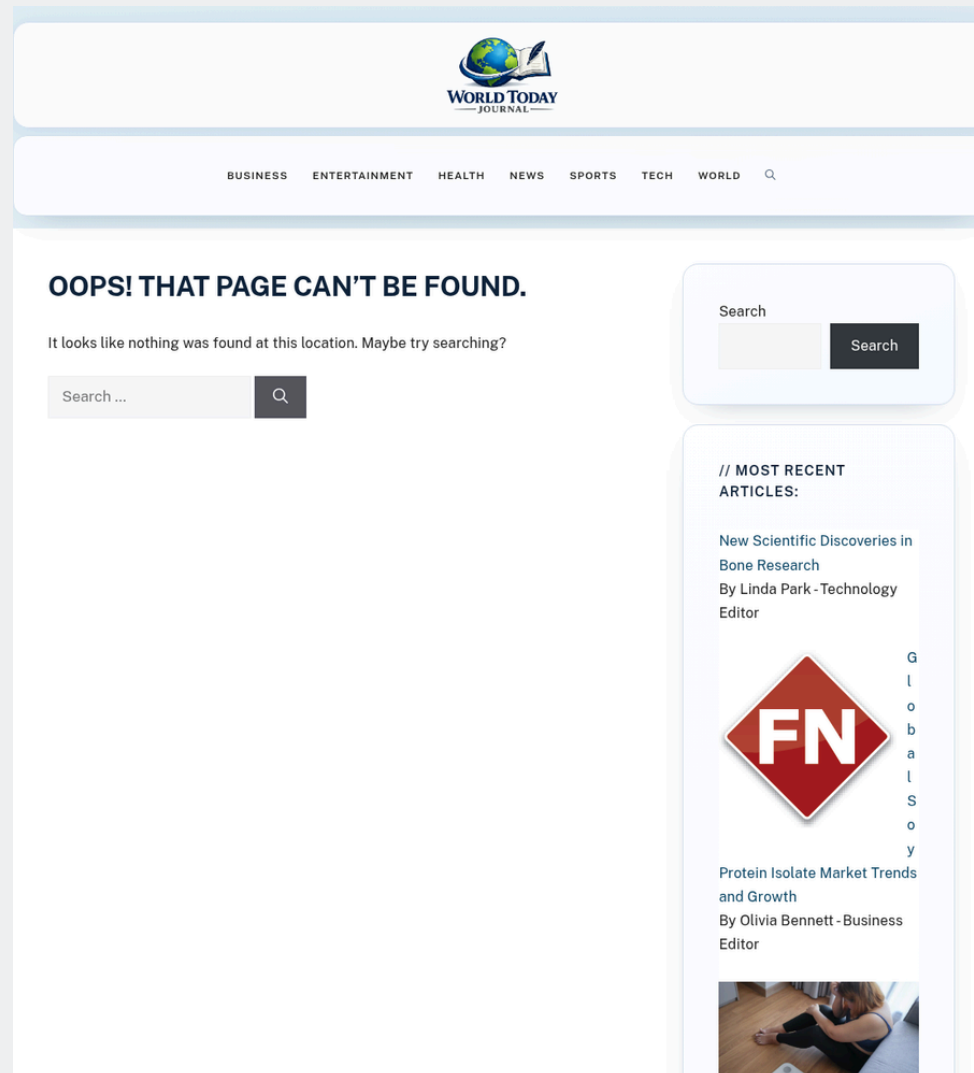
🌐 ONLINE

Page not found - World Today Journal

world-today-journal.com/why-cvss-scores...

Estimated Views

299





Global News Pakistan

Breaking Main Worldwide Pakistan Politics Health & Climate Entertainment Sports Technology News

24

Domain
Authority ?

Provided by
MOZ

182

Unique
Visits ?

Provided by
SimilarWeb

Apr 28, 2026 · ONLINE

News

National CERT launches first cyber training to boost...

globalnewspakistan.com/national-cert-lau...

Estimated Views

79



About

Contact

العربية اردو English

Opinion World wide Pakistan Politics Entertainment Health & Climate Technology Sports Blog

National CERT launches first cyber training to boost security

@ Sohail Majeed April 28, 2026 11:41 am



Islamabad (GNP) – National Cyber Emergency Response Team (National CERT) of Pakistan successfully organized a specialized cybersecurity capacity building training titled "FIRST Security Training Course" for its officials and technical resource persons at its headquarters.

The training was designed to further strengthen institutional readiness, enhance professional competencies, and reinforce operational resilience against evolving cyber threats.

Conducted under a Whole of Organization (WoO) Approach, the program brought together resources from National CERT's technical and operation tiers to build expertise in cybersecurity incident management and coordinated response.

The course covered key modules including FIRST Security Boot Camp, DDoS Mitigation Fundamentals and FIRST Threat Intelligence Pipelines. As the global Forum of Incident Response and Security Teams, FIRST is internationally recognized as the premier organization and global leader in incident response, making this training a significant step toward aligning National CERT's capabilities with international best practices.

The training was delivered by Muhammad Asad UI Rehman, National CERT's distinguished trainer, under the Distinguished Trainers Program (DTP). Participants demonstrated strong engagement and

Latest News



Islamic Philosophy is rooted in the Principles of Justice, Scholars



Rescuers Race Against Time as Venezuela Earthquake Toll Approaches 1,500



PM Expresses Grief Over Helicopter Crash in Saudi Arabia



Parliament Strengthens Democracy and Public Welfare, Speaker



Beyond Borders: The Missing Dimension in Conflict Resolution



Japan Plans to Invest \$210 Billion to Make Stronger Global Entertainment Leadership



Pakistan Digital Post

Flash Story Searching for the forgotten heroes of World War Two What's Scarier Than the Sex Talk? I...

4
Domain
Authority ?
Provided by
MOZ

56
Unique
Visits ?
Provided by
SimilarWeb

Pakistan Digital Post

The Pulse of Pakistan's Digital Future

- Home
- Digital Pakistan
- IT & Telecommunication
- AI
- Mobile Updates
- News
- About Us
- Privacy Policy
- Contact Us
- 🔍



Homepage / IT & Telecommunication /
National CERT Strengthens Cyber Defences with Advanced FIRST Security Training for Officials

IT & Telecommunication

National CERT Strengthens Cyber Defences with Advanced FIRST Security Training for Officials

Qaswar Abbas Zarkani April 28, 2026

Islamabad

Pakistan's cybersecurity preparedness has received a boost as the National CERT Pakistan conducted a specialised training programme aimed at enhancing institutional resilience against evolving digital threats.

Focus on Cyber Readiness

Recent Posts

- PTA Opens Door to Virtual Mobile
Operators in Major Telecom Market
Reform
- NCCIA Launches Probe Into Alleged
Disinformation Campaign Against
Easypaisa
- PTA Opens MVNO Licensing, Paving Way
for New Mobile Service Providers in
Pakistan
- Government Defends Telecom Bill,
Promises Changes to Address Legal
Concerns
- PM's Committee Proposes Major Changes
to Controversial Telecom Bill

Apr 28, 2026 · ONLINE

News

National CERT Strengthens Cyber Defences with...

pakistandigitalpost.com/national-cert-stre...

Estimated Views

48



IT Security Guru

48
Domain
Authority [?]
Provided by
MOZ

9.98K
Unique
Visits [?]
Provided by
SimilarWeb

[About Us](#)Monday, 29 June, 2026



HOMEFEATURESINSIGHTCHANNEL NEWSEVENTS TOPICSMULTIMEDIAPRODUCT REVIEWS

ABOUT US

Bridewell Joins Global Incident Response Network FIRST as Full Member

by [Guru Writer](#) — May 1, 2026 In News



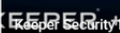
[Share on Facebook](#)[Share on Twitter](#)

Bridewell has been accepted as a full member of the Forum of Incident Response and Security Teams (FIRST), marking a significant milestone in the company's incident response maturity and global collaboration capabilities.

The UK-based cyber security services provider, which specialises in supporting critical national infrastructure (CNI) organisations, secured membership following a rigorous, peer-led vetting process and approval by the FIRST CSIRT Board of Directors. The achievement reflects Bridewell's ability to meet the high operational and trust standards required to join the global incident response community.

FIRST is an international organisation comprising more than 800 teams across over 100 countries, including government bodies, national CERTs, academic institutions

Recent News

**Keeper Security launches Microsoft Teams integration for privileged access management**

© JUNE 26, 2026

**UK Museums Are a Cyber Incident Waiting to Happen and the Government Knows It**

© JUNE 25, 2026

**New Forescout Data Reveals Slow Progress Toward Quantum-Safe Security**

© JUNE 24, 2026

**AI-Powered Phishing Attacks Surge 1,380% as Criminal Platforms Render MFA Obsolete**

© JUNE 24, 2026

May 01, 2026 ·  ONLINE

News

Bridewell Joins Global Incident Response Network FIRST as F...

itsecurityguru.org/2026/05/01/bridewell-j...

Estimated Views

463



UNDERCODE NEWS

Know the Threat Before It Strikes ⚡ It Finds You
👁️ It Hits Home 🏠 You Become the Target 🚫

26

Domain
Authority ?

Provided by
MOZ

1.19K

Unique
Visits ?

Provided by
SimilarWeb

May 01, 2026 · 🌐 ONLINE

News

Bridewell Joins FIRST: A Major Step Forward in Global Cyber...

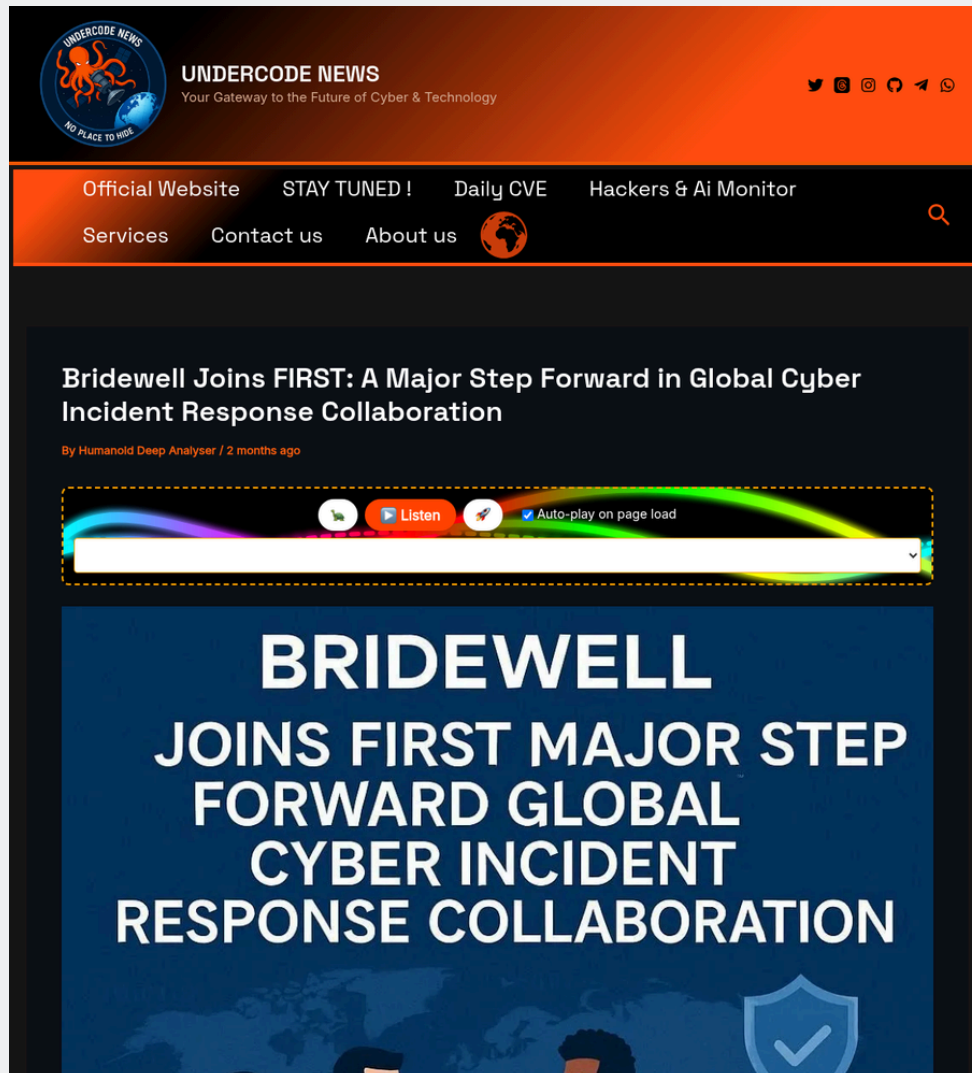
undercodenews.com/bridewell-joins-first-...

Estimated Views

368

Engagements

1





IT Security News

Cybersecurity news and articles about information security, vulnerabilities, exploits, hacks, laws, spam...

40
Domain
Authority ?

Provided by
MOZ

144
Unique
Visits ?

Provided by
SimilarWeb

May 01, 2026 · ONLINE

News

Bridewell Joins Global Incident Response Network FIRST as F...

itsecuritynews.info/bridewell-joins-global-...

Estimated Views

19

IT Security News

Cybersecurity news and articles about information security, vulnerabilities, exploits, hacks, laws, spam, viruses, malware, breaches.

Advertising Contact Legal and Contact information Opt-out preferences Privacy Policy Social Media

EN, IT SECURITY GURU

Bridewell Joins Global Incident Response Network FIRST as Full Member

2026-05-01 16:05

Bridewell has been accepted as a full member of the Forum of Incident Response and Security Teams (FIRST), marking a significant milestone in the company's incident response maturity and global collaboration capabilities. The UK-based cyber security services provider, which specialises in supporting critical national infrastructure (CNI) organisations, secured membership following a rigorous, peer-led vetting process [...]

The post [Bridewell Joins Global Incident Response Network FIRST as Full Member](#) appeared first on [IT Security Guru](#).

This article has been indexed from IT Security Guru

Read the original article:

[Bridewell Joins Global Incident Response Network FIRST as Full Member](#)

Share this:

Facebook X LinkedIn

Like this:

☆ Like Be the first to like this.

Related

[Bridewell research finds UK Financial Services under pressure from cyber security challenges and mounting regulatory requirements](#)

Research from Bridewell, a leading UK-based cyber security services provider, has found compliance with regulation as the chief challenge, as well as the main stimulus, for increasing cyber April 15, 2025 In "EN"

[Bridewell CEO gives cyber predictions for 2026](#)

As global economic pressures increase and budgets across both public and private sectors are cut, Anthony Young, CEO at Bridewell, a company that provides cybersecurity services to CNI November 19, 2025 In "EN"

[Bridewell and I-TRACING Form Strategic Partnership](#)

Today, I-TRACING and Bridewell, have announced a strategic partnership to create a strategic partnership to create the leading independent European cyber security services provider. The February 21, 2025 In "EN"

Search ...

PAGES

- [Advertising](#)
- [Contact](#)
- [Legal and Contact information](#)
- [Opt-out preferences](#)
- [Privacy Policy](#)
- [Social Media](#)
 - [Telegram Channel](#)

RECENT POSTS

- [Amazon Kindle E-Reader: Worth It, and How to Afford More Books?](#) June 29, 2026
- [Hackers Could Abuse WM_COPYDATA Callback Path to Execute Code Through Win32k Dispatch](#) June 29, 2026
- [ClawHub Skills Expose AI Agents to Remote Control Backdoors and Data Theft Attacks](#) June 29, 2026
- [Russia-Linked Turla Uses Compromised Infrastructure to Deploy STOCKSTAY in Ukraine Operations](#) June 29, 2026
- [OpenAI voluntarily limits new AI models at government's request](#) June 29, 2026
- [Beyond the perimeter: The shift to data-centric protection](#) June 29, 2026
- [DOJ Seizes 400 Illegal FIFA](#)



Best African News Online

Zimbabwe news , newsdzezimbabwe with spiked catch all breaking news on 24news online media...

30

Domain
Authority ?

Provided by
MOZ

2.01K

Unique
Visits ?

Provided by
SimilarWeb

May 07, 2026 · ONLINE

News

POTRAZ, FIRST Technical Colloquium 2026: Africa...

spikedmedia.co.zw/potraz-first-technical-...

Estimated Views

684

Engagements

1

Sunday, June 28, 2026 3:41:17 PM

SPIKED.
Fresh Unbiased Viewpoint

Best African News
Online

LATEST NEWS

HOME LIFESTYLE HEALTH TOURISM & TRAVEL SPORTS MUSIC POLITICS

COMMUNITY BUSINESS

Home » Business » POTRAZ, FIRST Technical Colloquium 2026: Africa Sharpens Its Cyber Edge

BUSINESS DEVELOPMENT SCIENCE AND TECHNOLOGY

POTRAZ, FIRST Technical Colloquium 2026: Africa Sharpens Its Cyber Edge

Byron Adonis Mutingwende 2 Months Ago 0 6 Mins

Against the thundering backdrop of Victoria Falls, one of the natural world's most commanding spectacles, a quieter but no less consequential gathering is taking shape this week inside the Kalundu Room of Elephant Hills Resort.

Search Here

Search ...

SEARCH

CONGRATULATIONS ZIMBABWE
Celebrating Zimbabwe's Election to the United Nations Security Council

SAY NO TO



Tenable®

The leader in exposure management and AI security, Tenable cybersecurity solutions reduce...

76

Domain Authority ?

Provided by
MOZ

422K

Unique Visits ?

Provided by
SimilarWeb

tenable

Platform Solutions Why Tenable Resources Company Pricing Buy Try

BLOG RESEARCH

10-minute read May 8 2026

Why the approaching flood of vulnerabilities changes everything — and what to do about it

By Raymond Carney

in reddit x share Subscribe

tenable research
special operations

May 08, 2026 · ONLINE

Comment

Why the approaching flood of vulnerabilities changes everything ...

tenable.com/blog/why-the-approaching-fl...

Estimated Views

3.87K

Engagements

9



Security Boulevard

Security Boulevard is home of the Security Bloggers Network (SBN). A single source for news, analysis ...

70
Domain
Authority [?]

Provided by
MOZ

71.5K
Unique
Visits [?]

Provided by
SimilarWeb

May 08, 2026 · ONLINE

Feature

Why the approaching flood of vulnerabilities changes everything ...

securityboulevard.com/2026/05/why-the-...

Estimated Views

533

Monday, June 29, 2026

Security Boulevard
POWERED BY **Techstrong | Group**
a **Futurum** company

Home ▾ Security Creators Network ▾ Webinars ▾ Events ▾ Sponsored Content ▾ Chat ▾ Library ▾ Related Sites ▾ Media Kit ▾ About ▾

ANALYTICS APPSEC CISO CLOUD DEVOPS GRC IDENTITY INCIDENT RESPONSE IOT / ICS THREATS / BREACHES MORE ▾

HUMOR

Home » Security Bloggers Network » Why the approaching flood of vulnerabilities changes everything — and what to do about it

Why the approaching flood of vulnerabilities changes everything — and what to do about it
by Raymond Carney on May 8, 2026

The post [Why the approaching flood of vulnerabilities changes everything — and what to do about it](#) appeared first on [Tenable Blog](#).

AI-driven discovery, NIST's retreat from universal enrichment, and the end of "good enough" vulnerability management

Key takeaways

1. AI-driven discovery tools are accelerating CVE volume, resulting in an expected deluge of 59,000 disclosed vulnerabilities this year.
2. NIST has dramatically scaled back enrichment of CVEs in the National Vulnerability Database (NVD), which will leave most new vulnerabilities without the critical metadata and severity scores required for traditional automated prioritization and patching.
3. Tenable customers aren't impacted by these developments because our exposure intelligence infrastructure hasn't depended upon NVD enrichment for years.

Three things happened in April 2026 that, taken together, represent the most significant shift in the [vulnerability management](#) landscape in over a decade. If you're still relying on hybrid methods — spreadsheets alongside scanners, manual triage stacked on top of automated feeds, hope as a strategy — these developments deserve your full attention.

The new vulnerability management landscape

On April 7, Anthropic launched [Project Glasswing](#), a cybersecurity initiative built on its Claude Mythos frontier AI model. The premise: frontier AI can discover zero-day vulnerabilities in software at a speed

Techstrong TV

LIVE Unmute broadcast
Click full-screen to enable volume control
Watch latest episodes and shows

Tech Field Day Events

36:29 AI INFRASTRUCTURE

Upcoming Webinars

ADR vs. EDR: Isn't Enough in the AI Era
REGISTER NOW
AUGUST 12, 2026 3:00 PM EDT

Podcast

Security Boulevard Podcast



TechnoMag

41

Domain
Authority ?

Provided by
MOZ

2.14K

Unique
Visits ?

Provided by
SimilarWeb

May 08, 2026 · ONLINE

News

Cyber Resilience Takes Center Stage at POTRAZ Technical...

technomag.co.zw/cyber-resilience-takes-...

Estimated Views

330



AFRICA TECH NEWS BUSINESS CURRENT NEWS LOCAL TECH NEWS TECH TECH NEWS

Cyber Resilience Takes Center Stage at POTRAZ Technical Colloquium

By GANUCHIRAI MAPAKO · May 8, 2026



The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) Technical Colloquium, held in partnership with the Forum of Incident Response and Security Teams (FIRST), has shifted into high gear with an intensive live cyber drill placing cybersecurity at the forefront as a pillar of national and economic stability.

The gathering brought together 100 cybersecurity experts from across Africa for an intensive live cyber drill, a hands-on exercise simulating real-world attacks including ransomware outbreaks, phishing campaigns, and infrastructure breaches. Participants tested their ability to detect, respond to, and recover from incidents in a controlled, high-stakes environment.



Dark Reading

Dark Reading: Connecting The Cybersecurity Community.

82
Domain Authority 
Provided by 

194K
Unique Visits 
Provided by 

[Informa TechTarget](#)
[SearchSecurityCybersecurity.DiveInformationWeekChannel.Dive](#)
[Explore our brandsAn Informa TechTarget Publication](#)
[Dark Reading Resource LibraryBlack Hat NewsOmdia CybersecurityAdvertise](#)



[Newsletter Sign-Up](#)
[Newsletter Sign-Up](#)

Cybersecurity Topics

Related Topics

- [Application Security](#)
- [Cybersecurity Careers](#)
- [Cloud Security](#)
- [Cyber Risk](#)
- [Cyberattacks & Data Breaches](#)
- [Cybersecurity Analytics](#)
- [Cybersecurity Operations](#)
- [Data Privacy](#)
- [Endpoint Security](#)
- [ICS/OT Security](#)
- [Identity & Access Mgmt Security](#)
- [Insider Threats](#)
- [IoT](#)
- [Mobile Security](#)
- [Perimeter](#)
- [Physical Security](#)
- [Remote Workforce](#)
- [Threat Intelligence](#)
- [Vulnerabilities & Threats](#)

Recent in Cybersecurity Topics



May 12, 2026 ·  ONLINE Roundup

20 Leaders Who Built the CISO Era: 2 Decades of Change

darkreading.com/cybersecurity-operation...

Estimated Views **933**



World Today Journal

World Today Journal delivers breaking world news, business, technology, sports, health and...

40

Domain
Authority ?

Provided by
MOZ

2.14K

Unique
Visits ?

Provided by
SimilarWeb

May 13, 2026 · ONLINE

News

AI-Powered Cyberattacks Exposed: How Goog...

world-today-journal.com/ai-powered-cyb...

Estimated Views

299



BUSINESS ENTERTAINMENT HEALTH NEWS SPORTS **TECH** WORLD



AI-POWERED CYBERATTACKS EXPOSED: HOW GOOGLE STOPPED THE FIRST AI- GENERATED HACK-AND WHY THOUSANDS MORE ARE COMING WITHOUT WARNING

May 13, 2026 by Linda Park - Technology Editor

GOOGLE THWARTS FIRST MAJOR AI-POWERED CYBERATTACK: THE NEW ERA OF DIGITAL THREATS

By Linda Park | Technology Editor | May 13, 2026 | San Francisco, USA

In a landmark disclosure that signals a seismic shift in cybersecurity, Google has confirmed thwarting the first known **AI-generated zero-day cyberattack**, where hackers used machine learning models to autonomously discover and exploit previously unknown vulnerabilities in software. The incident, which security researchers describe as a "watershed moment," raises urgent questions about whether current defenses can keep pace with an arms race where artificial intelligence itself becomes both the weapon and the architect of digital warfare.

Search

Search

// MOST RECENT
ARTICLES:

New Scientific Discoveries in
Bone Research
By Linda Park - Technology
Editor



Global
Society

Protein Isolate Market Trends
and Growth
By Olivia Bennett - Business
Editor





INCYBER NEWS

Le média de la confiance numérique

42

Domain
Authority [?]

Provided by
MOZ

11.3K

Unique
Visits [?]

Provided by
SimilarWeb



May 25, 2026 · ONLINE

Feature

Pourquoi Mythos signe la fin du patch management...

incyber.org/article/pourquoi-mythos-signe...

Estimated Views

1.48K

Engagements

1

CSO

CSO Online

CSO delivers the critical information about trends, practices, and products enterprise security leaders...

84

Domain
Authority ?

Provided by
MOZ

165K

Unique
Visits ?

Provided by
SimilarWeb

Jun 23, 2026 · ONLINE

News

CISA tells agencies to patch smarter, not harder —...

csoonline.com/article/4183750/cisa-tells-...

Estimated Views

678

Engagements

6

CSO



Home • Security • Security Software • Threat and Vulnerability Management

by Cynthia Brumfield
Contributing Writer



CISA tells agencies to patch smarter, not harder — foreshadowing broader industry practice

News Analysis
Jun 10, 2026 • 10 mins

A new CISA directive moves federal agencies beyond severity scores and toward a risk-based patching model that prioritizes real-world exploitation, asset exposure, and attacker impact — a framework many security leaders see as the future of vulnerability management.



Credit: jackpress / Shutterstock



Trend – News from Azerbaijan, Georgia, Kazakhstan, Turkmenistan, Uzbekistan, Iran and Turkey.

Trend News Agency is a leading news provider from the Caucasus, Caspian and Central Asian regions....

77
Domain
Authority 
Provided by
MOZ

139K
Unique
Visits 
Provided by
SimilarWeb

Jun 11, 2026 ·  ONLINE

News

Azerbaijan's FinCERT joins global cybersecurity netwo...

trend.az/business/4196641.html

Estimated Views

830

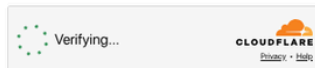
Engagements

1

www.trend.az

Performing security verification

This website uses a security service to protect against malicious bots. This page is displayed while the website verifies you are not a bot.





ProPakistani

ProPakistani is the premier and most trustworthy resource for all happenings in technology, telecom...

74

Domain Authority ?

Provided by
MOZ

2.03M

Unique Visits ?

Provided by
SimilarWeb

PROPRICE LENS HOWTO TOOLS 4G,5G & INTERNET PACKAGES CAREERS ABOUT CONTACT US

propakistani



Pakistan Becomes Full Member of Elite Global Cybersecurity Club

By Business Desk | Published Jun 8, 2026 | 6:30 pm



The Pakistan National Cyber Emergency Response Team (PKCERT) has been accepted as a Full Member of the Forum of Incident Response and Security Teams (FIRST), marking a major milestone in Pakistan's growing presence in the global cybersecurity landscape.



This achievement places Pakistan's national cyber defense body within an elite international network of trusted incident response teams.

Latest News

Instagram Tests More Ways to Let Users Control Their Algorithm



PUBG MOBILE and Naruto Shippuden Partner For One Of The Most Ambitious...



Member Assembly Caught Vanishing on Floor of the



ALSO READ

Jun 08, 2026 · ONLINE

News

Pakistan Becomes Full Member of Elite Global Cybersecurit...

propakistani.pk/2026/06/08/pakistan-be...

Estimated Views

17.9K

Engagements

2



Help Net Security

Cybersecurity news with a focus on enterprise security. Discover what matters in the world of...

76

Domain
Authority ?

Provided by
MOZ

209K

Unique
Visits ?

Provided by
SimilarWeb

Jun 15, 2026 · ONLINE

News

AI vulnerability discovery is pushing 2026 CVEs toward...

[helpnetsecurity.com/2026/06/15/first-2026...](https://helpnetsecurity.com/2026/06/15/first-2026-cve-forecast/)

Estimated Views

1.28K

Engagements

9

Help Net Security newsletters: Daily and weekly news, cybersecurity jobs, open source projects, breaking news – [subscribe here!](#)

HELPNETSECURITY
News Features CISO AI Videos Product showcase Industry news Reviews Whitepapers Events Newsletters

Hidden identities create hidden risk.
How do you achieve full visibility?
[GET THE CISO GUIDE](#)

Mirko Zorz, Director of Content, Help Net Security
June 15, 2026
AI vulnerability discovery is pushing 2026 CVEs toward 66,000
Share

Vulnerability disclosures are piling up faster in 2026 than anyone expected at the start of the year. The running count for the first few months sits well above the original projection, and the Forum of Incident Response and Security Teams (FIRST) now expects the year to land near 66,000 CVEs.

The cause sits mostly with one development: **AI tools** have started hunting for software flaws on their own, and they are good at it.

"The teams that will weather the vulnerability storm of 2026 are the ones with trusted networks already in place, who are sharing intelligence and are coordinating response before any crises hit," said **Chris Gibson**, CEO of FIRST.

The machines doing the hunting

Autonomous discovery agents are now part of the disclosure ecosystem. Anthropic's **Mythos**, and OpenAI's **GPT-5.4-Cyber** have pushed up the volume of flaws being found.

Featured news

- DarkMoon: Open-source AI pentesting platform
- Synology issues critical fix for MailPlus Server vulnerabilities
- Mystery hackers use novel SharkLoader dropper against governments, software devs

Resources

- Download: Secure Foundations for AI Workloads on AWS
- Download: Automating Pentest Delivery Guide
- CIS Benchmarks March 2026 Update



Mastodon hosted on mastodon.social

The original server of Mastodon, operated by Mastodon GmbH for the common good.

82

Domain
Authority [?]

Provided by
MOZ

845K

Unique
Visits [?]

Provided by
SimilarWeb

Feb 07, 2025 ·  ONLINE

The page you are looking for isn't here. - Mastodon

mastodon.social/@campuscodi/11675985...



The page you are looking for isn't here.

Estimated Views

5.45K

B/C

BornCity

BornCity - Ihr IT-Newsportal: Aktuelle Windows-News, Sicherheitswarnungen, Software-Updates...

60

Domain Authority ?

Provided by MOZ

309K

Unique Visits ?

Provided by SimilarWeb

Jun 15, 2026 · ONLINE

News

Cybersicherheit 2026: 66.000 Sicherheitslücken u...

borncity.com/news/cybersicherheit-2026-...

Estimated Views

3.36K

BORN/CITY TECHNOLOGIE SICHERHEIT SOFTWARE HARDWARE MOBILE KI ROBOTIK ÜBER UNS

Sicherheit Cybersicherheit Künstliche Intelligenz Regulierung Technologie

Cybersicherheit 2026: 66.000 Sicherheitslücken und KI-Würmer

Die Zahl erwarteter Schwachstellen steigt drastisch, während selbstreplizierende KI-Würmer neue Risiken für Unternehmen schaffen.

BornCity Redaktion · 15.06.2026, 17:18 Uhr



DIE KERNPUNKTE

- Prognose von 66.000 Sicherheitslücken
- Autonome KI-Würmer bedrohen Netzwerke
- 72 Prozent mehr KI-Cyberfälle weltweit
- CISA ordnet autonome Schadensbehebung an

Künstliche Intelligenz treibt einen Wettlauf zwischen Angreifern und Verteidigern an, der sich rasant beschleunigt. Neue Daten zeigen einen dramatischen Anstieg automatisierter Bedrohungen – während gleichzeitig Regulierungsbehörden auf...

Meistgelesene Artikel

- AirPods Pro 3: Rekordtief bei 161 Euro mit Herzfrequenz-Sensor**
Gestern, 20:46 Uhr
- RTX 5090: NVIDIA-Grafikkarte erreicht 14.073 Token-Durchsatz**
Gestern, 20:01 Uhr
- AirPods-Protokoll geknackt: Schüler ermöglicht Android-Zugang**
Heute, 00:50 Uhr
- iPhone 18: Apple plant 200-Euro-Preisaufschlag für September**
Heute, 06:35 Uhr
- iPhone 18 Pro und erstes Foldable: Apple-Event im September**
Heute, 09:40 Uhr
- Steam Machine: Bastler bauen günstige Alternativen für 700 Euro**
Gestern, 23:00 Uhr
- Grok 4.5: Musks KI-Modell mit 1,5 Billionen Parametern startet**
Gestern, 18:00 Uhr
- macOS-Tools: Sechs neue Produktivitäts-Apps am 28. Juni**
Gestern, 21:22 Uhr
- MacBook Ultra: Apple bringt Touchscreen und OLED-Display**
Gestern, 16:40 Uhr
- Vera-Rubin-Plattform: Nvidias neuer Standard kommt im Herbst**
Heute, 00:23 Uhr

Mehr zum Thema Technologie

- Google Slides: KI-Workflow wandelt Excel-Daten in Folien...**
Heute, 15:12 Uhr



cyberdefensewire.com

26
Domain
Authority [?]
Provided by
MOZ

2.36K
Unique
Visits [?]
Provided by
SimilarWeb

🌐 ONLINE

News

FIRST Mid-Year Vulnerability Forecast Confirms Historic...

cyberdefensewire.com/first-mid-year-vuln...

Estimated Views

1K

Call us Toll Free (USA): 1-833-844-9468 International: +1-603-280-4451 M-F 8am to 6pm EST

Cyber Defense Magazine Cyber Defense Awards Cyber Defense Webinars Cyber Defense Conferences Cyber Defense TV Cyber Defense Radio Subscribe

CYBERDEFENSE^{Wire} Home Press Releases Contact [Submit a Press Release](#)

FIRST Mid-Year Vulnerability Forecast Confirms Historic Surge, Projects ~66,000 CVEs in 2026

in [Twitter](#) [Facebook](#) [Email](#) [+](#)

AI and a rapidly expanding CVE ecosystem blow past February's already-record projections by 46%, but exploitable risk remains flat

DENVER, June 15, 2026 – Today at **FIRST's 38th Annual Conference**, the Forum of Incident Response and Security Teams (**FIRST**) released its 2026 Mid-Year Vulnerability Forecast, revealing that actual CVE disclosures are already running 46.3% above the projections published just four months ago.

A mid-year reassessment shows disclosures are climbing faster than initially predicted. The updated 2026 forecast now projects approximately ~66,000 CVEs for the full year, up from the **February median of 59,427**, marking the first time in history that annual vulnerability disclosures are on pace to approach 70,000. The surge reflects more aggressive security research and better reporting practices, not a decline in software security itself.

"We're witnessing a major shift in the vulnerability landscape. Not because software is suddenly less secure, but because our collective ability to find flaws has been structurally transformed," said **Éireann Leverett**, FIRST Liaison and Lead Member of FIRST's Vulnerability Forecasting Team. "The challenge for defenders is no longer the discovery of vulnerabilities; it's the capacity to verify, coordinate, and prioritize them at a scale the industry has never seen before."

Key Findings from FIRST's 2026 Mid-Year Vulnerability Forecast

- Cumulative drift of +46.3% above the February forecast, with 6,120 excess CVEs

Press Release by Forum of Incident Response and Security Teams (FIRST)

Media Contact

Summer Mitchell
summer@growthstackmedia.com

Cyber Defense Magazine
June Edition for 2026

[Download eMag](#)

Published monthly by Cyber Defense Magazine, this resource shares a wealth of information to help you stay one step ahead of the next cyber threat.





SecurityBrief US

SecurityBrief US is focused on cybersecurity and cyberattack news. Its readers include business an...

29

Domain
Authority ?

Provided by
MOZ

214

Unique
Visits ?

Provided by
SimilarWeb

Jun 19, 2026 · ONLINE

News

FIRST raises 2026 vulnerability forecast to 66,000 CVEs

securitybrief.news/story/first-raises-2026-...

Estimated Views

65

SecurityBrief US - Technology news for CISOs & cybersecurity decision-makers

SecurityBrief
UNITED STATES

POWERED BY
TechDay

GUIDES

Cloud Security Cybersecurity Endpoint Protection Firewalls Ransomware

Search...



SOCS AI CYBERSECURITY

FIRST raises 2026 vulnerability forecast to 66,000 CVEs

Thu, 18th Jun 2026

Image: Jerry Gamblin

Related stories

- Reducing cyber risk is still hard: Why CTEM stalls at action
- Silent Push 6.0 adds AI workflows and unified cyber platform
- Reco launches agent security for enterprise AI risk
- Netwrix adds AI governance to 1Secure for Microsoft
- Cynomi adds automation & AI for MSP vulnerability work

Top stories

- Cisco and OpenAI outline AI's growing role in cyber defence

**SOFIAH NICHOLE SALIVIO**
News Editor

FIRST has raised its 2026 vulnerability disclosure forecast to about 66,000 CVEs after a mid-year update from the incident response and security body.

Common Vulnerabilities and Exposures disclosures are running 46.3% above the level projected earlier this year, with 6,420 more CVEs recorded through April than expected under the previous model.

That would put 2026 close to 70,000 published vulnerabilities, up from a February median forecast of 59,427, and mark a historic high in annual disclosure volume.

Researchers behind the forecast said the rise does not point to a broad deterioration in software quality. Instead, they attributed it to changes in how flaws are found and reported.

The main factors were AI-assisted vulnerability discovery, a 449% year-on-year rise in GitHub Security Advisory volume, and a 3,119% increase in activity from VulnCheck as a CVE Numbering Authority handling previously unassigned vulnerabilities.

The report also found that the number of distinct software products with tracked vulnerabilities has grown by two orders of magnitude, increasing the workload for security teams even where exploitability levels remain stable.

securityonline.info/2026-vulnerability-for...



LinkedIn

1 billion members | Manage your professional identity. Build and engage with your professional network. Access knowledge, insights and opportunities.

LINKEDIN

LinkedIn Login, Sign in | LinkedIn

linkedin.com/uas/login?session_redirect=...



Sign in

New to LinkedIn? [Join now](#)



Continue with Google



Sign in with Apple

By continuing, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

or

Email or phone

Password



[Forgot password?](#)



Keep me signed in

Sign in

LinkedIn Corporation © 2026 [User Agreement](#) [Privacy Policy](#) [Community Guidelines](#) [Cookie Policy](#) [Copyright Policy](#) [Send Feedback](#) [Language](#) ▼



Access denied | drj.com used Cloudflare to restrict access | drj.com | Cloudflare

50
Domain
Authority [?]
Provided by
MOZ

9.7K
Unique
Visits [?]
Provided by
SimilarWeb

DRJ FALL 2026
Sept. 27-30 Dallas

RESILIENCE IN MOTION

Moving Your Program Forward

75

SECURITY

DISASTER RECOVERY

DRJOURNAL

EN ESPAÑOL | SIGN IN |
SUBSCRIBE

Q Search the Journal

THE JOURNAL

EVENTS

WEBINARS

MENTOR PROGRAM

RESOURCES

ABOUT

FIRST Mid-Year Vulnerability Forecast Confirms Historic Surge, Projects ~66,000 CVEs in 2026

June 22, 2026

AI and a rapidly expanding CVE ecosystem blow past February's already-record projections by 46%, but exploitable risk remains flat

DENVER – Today at **FIRST's 38th Annual Conference**, the Forum of Incident Response and Security Teams (**FIRST**) released its 2026 Mid-Year Vulnerability Forecast, revealing that actual CVE disclosures are already running 46.3% above the projections published just four months ago.

A mid-year reassessment shows disclosures are climbing faster than initially predicted. The updated 2026 forecast now projects approximately ~66,000 CVEs for the full year, up from the **February median of 59,427**, marking the first time in history that annual vulnerability disclosures are on pace to approach 70,000. The surge reflects more aggressive security research and better reporting practices, not a decline in software security itself.

"We're witnessing a major shift in the vulnerability landscape, not because software is suddenly less secure, but because our collective ability to find flaws has been structurally transformed," said **Fioreann Leverett**, FIRST Liaison and

Recent Posts

Noma Partners With Kong to Secure the Agentic AI Era
June 26, 2026

New NACCHO Research Describes Strengths, Challenges in Local Health Department Preparedness and Response Capacity
June 25, 2026

ControlMonkey Expands Cyber Resilience Platform With Data Backup Correlation
June 25, 2026

Keeper Security Brings Privileged Access Controls to Microsoft Teams With New Keeper Teams App
June 25, 2026

Secureframe Insights Offer Blueprint to Strengthen Federal Cybersecurity
June 25, 2026

Jun 22, 2026 · ONLINE

Access denied | drj.com used Cloudflare to restric...

drj.com/industry_news/first-mid-year-vuln...

Estimated Views

152

Engagements

1



Dark Reading

Dark Reading: Connecting The Cybersecurity Community.

82

Domain Authority ?

Provided by
MOZ

194K

Unique Visits ?

Provided by
SimilarWeb

SearchSecurityCybersecurity DiveInformationWeekChannel Dive

Explore our brands

Dark Reading Resource LibraryBlack Hat NewsOmdia CybersecurityAdvertise

Dark Reading

NEWSLETTER SIGN-UP

Cybersecurity TopicsWorldThe EdgeDR TechnologyEventsResources

CYBERSECURITY OPERATIONSAPPLICATION SECURITYCYBER RISKEndpoint SecurityNEWS

AI Decline? Confidence in Autonomous Penetration Testing Falls

Companies are still experimenting with automated AI systems to find security weaknesses, but fewer are relying on the technology.

Robert Lemos, Contributing Writer
June 26, 2026

5 Min Read

Editor's Choice

SOURCE: ASMAULNA VIA SHUTTERSTOCK

in

f

X

reddit

twitter

email

In 2025, nearly 3 in 10 security professionals thought that fully autonomous AI systems could satisfy their companies' security-testing needs. But after a year of testing and experimentation, that optimism has largely gone away.

CYBERSECURITY OPERATIONS

DARK READING
CONFIDENTIAL

Do CISOs Need a Code of Ethics?

by Dark Reading Editorial Team

JUN 24, 2026

CYBERSECURITY OPERATIONS

2026 FIFA World Cup Faces Surge in Cyber Threats

by Alexander Culafi

JUN 24, 20263 MIN READ

Jun 26, 2026 · ONLINE

News

AI Decline? Confidence Falls in Autonomous...

darkreading.com/cybersecurity-operation...

Estimated Views

933



Security Boulevard

Security Boulevard is home of the Security Bloggers Network (SBN). A single source for news, analysis ...

70
Domain
Authority [?]

Provided by
MOZ

71.5K
Unique
Visits [?]

Provided by
SimilarWeb

Jun 22, 2026 · ONLINE

News

Report: CVE Disclosures Are 46% Higher Than...

[securityboulevard.com/2026/06/report-c...](https://securityboulevard.com/2026/06/report-cve-disclosures-are-46-percent-higher-than-projected-in-first-half-of-2026/)

Estimated Views

533

Monday, June 29, 2026

Security Boulevard
POWERED BY **Techstrong | Group**
a **Futurum** company

Home ▾ Security Creators Network ▾ Webinars ▾ Events ▾ Sponsored Content ▾ Chat ▾ Library ▾ Related Sites ▾ Media Kit ▾ About ▾

ANALYTICS APPSEC CISO CLOUD DEVOPS GRC IDENTITY INCIDENT RESPONSE IOT / ICS THREATS / BREACHES MORE ▾

HUMOR

Home » Security Boulevard (Original) » Report: CVE Disclosures Are 46% Higher Than Projected in First Half of 2026

Report: CVE Disclosures Are 46% Higher Than Projected in First Half of 2026

by Michael Vizard on June 22, 2026

A report published by the Forum of Incident Response and Security Teams (FIRST), a nonprofit organization for incident response professionals, finds that the rate at which Common Vulnerabilities and Exposures (CVE) are being disclosed in the first half of 2026 is 46% higher than initially projected.

FIRST is now projecting there will be approximately 66,000 CVEs disclosed in 2026, up from the 59,427 that were initially forecasted in February.

Éireann Leverett, lead member of the vulnerability forecasting team at FIRST, said it's not possible to conclusively determine to what degree artificial intelligence (AI) is affecting the rate of increased CVE discovery, but it is a likely factor. The Mozilla CVE Naming Authority (CNA), for example, reported a 164% spike in Q1 CVE disclosures that are directly attributable to AI-assisted tooling running against the Firefox engine.

However, there are also other factors, including a 449% year-over-year surge in GitHub Security Advisory (GHSAs) volume, and a 3,119% increase in the size of the VulnCheck CVE Naming Authority (CNA) backlog of unassigned vulnerabilities that have not been assigned to a single vendor.

As of yet, the report notes that vulnerabilities that are actively exploited or credibly exploitable have not risen at the same rate. Nevertheless, it has been shown that once a CVE is discovered, the amount of time that cybercriminals require to reverse engineer an exploit in the age of AI is now measured in hours versus weeks.

Jerry Gamblin, co-author of the forecast and FIRST EPSS SIG member, said cybersecurity teams should also keep in mind that not all CVEs reported are of equal severity. AI tools tend to often generate AI slop that, while similar to the vulnerabilities a human might discover, are not always relevant, he added. There is also still a tendency to over-inflate the severity ranking of a CVE whenever researchers factor in a worst-case scenario. The issue, of course, is that cybersecurity and IT teams still need to allocate time and resources to investigate CVEs.

Techstrong TV

Click full-screen to enable volume control
Watch latest episodes and shows

Tech Field Day Events

Upcoming Webinars

Podcast



Bank information security news, training, education - BankInfoSecurity

BankInfoSecurity.com is your source for banking
information security related content, including frau...

72
Domain
Authority 
Provided by
MOZ

63K
Unique
Visits 
Provided by
SimilarWeb

Jun 23, 2026 ·  ONLINE

News

FortiBleed Is 'Tip of the Iceberg' of Edge Device Targeting

bankinfosecurity.com/fortibleed-tip-iceber...

Estimated Views

479

Engagements

2

ISMG Network ▾USA ▾

Sign InRegisterCyberEd.io Catalog



Topics ▾News ▾Training ▾Resources ▾Events ▾Jobs ▾

TRENDING: The Cybersecurity Skills Gap and the Role of AI for Defenders · Modernizing at Speed: Scaling AI and Apps Without New Silos ·

Cybercrime , Fraud Management & Cybercrime , Network Firewalls, Network Access Control

FortiBleed Is 'Tip of the Iceberg' of Edge Device Targeting

Threat Actor Harvesting Other Credentials; Experts See Many More Scans for SSL-VPNs

Mathew J. Schwartz (@euroinfosec) · June 23, 2026

 Share Post Share★ Credit Eligible

Get Permission



Image: Shutterstock/ISMG

The Fortinet credential-harvesting feeding frenzy being tracked as "FortiBleed" is just one of many active, illicit efforts targeting edge devices built by a range of

GET DAILY EMAIL UPDATES

Covering topics in risk management, compliance, fraud, and information security.

Submit

By submitting this form you agree to our [Privacy & GDPR Statement](#)

RESOURCES

[whitepaper](#)
New Attacks. Skyrocketing Costs. The True Cost of a Security Breach.

[whitepaper](#)
Top Three Cyber Predictions for 2025

[whitepaper](#)
Corelight's Brian Dye on NDR's Role in Defeating Ransomware

[whitepaper](#)
Defeat Ransomware: Free Readiness Guide

[whitepaper](#)
Cloud NGFW : Best-in-class security and unparalleled simplicity on AWS

A

Digital Security Authority

Digital Security Authority (digitalsecurityauthority.com) is a national-scope reference directory covering the cybersecu

12

Domain
Authority ?

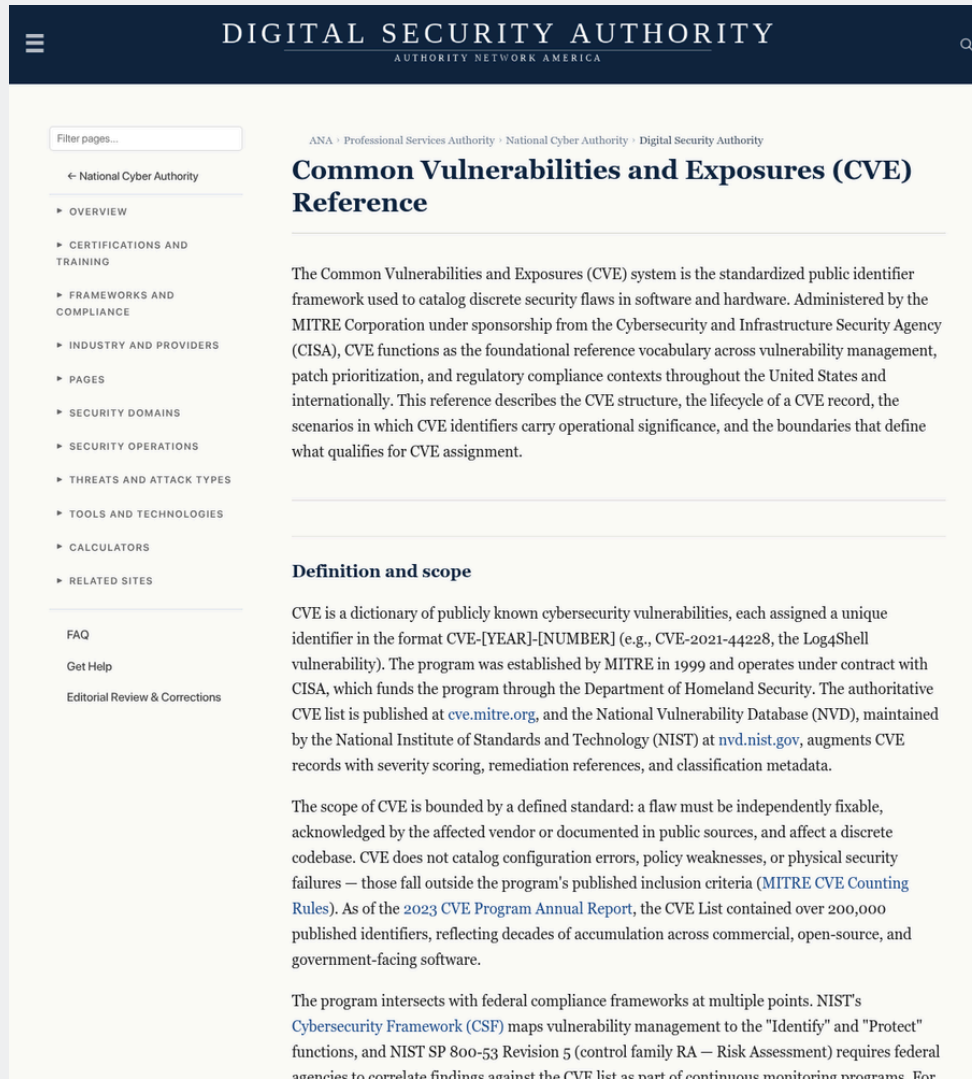
Provided by
MOZ

Mar 12, 2026 ·  ONLINE

Feature

Common Vulnerabilities and Exposures (CVE)...

digitalsecurityauthority.com/common-vuln...



The screenshot shows the Digital Security Authority website. The header is dark blue with the text 'DIGITAL SECURITY AUTHORITY' and 'AUTHORITY NETWORK AMERICA'. A search icon is on the right. A left sidebar contains a 'Filter pages...' search bar and a list of navigation links: '← National Cyber Authority', 'OVERVIEW', 'CERTIFICATIONS AND TRAINING', 'FRAMEWORKS AND COMPLIANCE', 'INDUSTRY AND PROVIDERS', 'PAGES', 'SECURITY DOMAINS', 'SECURITY OPERATIONS', 'THREATS AND ATTACK TYPES', 'TOOLS AND TECHNOLOGIES', 'CALCULATORS', 'RELATED SITES', 'FAQ', 'Get Help', and 'Editorial Review & Corrections'. The main content area is titled 'Common Vulnerabilities and Exposures (CVE) Reference' and includes a breadcrumb trail: 'ANA > Professional Services Authority > National Cyber Authority > Digital Security Authority'. The text describes the CVE system as a standardized public identifier framework used to catalog discrete security flaws in software and hardware, administered by the MITRE Corporation under sponsorship from the Cybersecurity and Infrastructure Security Agency (CISA). It details the CVE structure, lifecycle, and operational significance. A section titled 'Definition and scope' explains that CVE is a dictionary of publicly known cybersecurity vulnerabilities, each assigned a unique identifier in the format CVE-[YEAR]-[NUMBER] (e.g., CVE-2021-44228, the Log4Shell vulnerability). It notes that the program was established by MITRE in 1999 and operates under contract with CISA, which funds the program through the Department of Homeland Security. The authoritative CVE list is published at cve.mitre.org, and the National Vulnerability Database (NVD), maintained by the National Institute of Standards and Technology (NIST) at nvd.nist.gov, augments CVE records with severity scoring, remediation references, and classification metadata. The scope of CVE is bounded by a defined standard: a flaw must be independently fixable, acknowledged by the affected vendor or documented in public sources, and affect a discrete codebase. CVE does not catalog configuration errors, policy weaknesses, or physical security failures — those fall outside the program's published inclusion criteria ([MITRE CVE Counting Rules](#)). As of the [2023 CVE Program Annual Report](#), the CVE List contained over 200,000 published identifiers, reflecting decades of accumulation across commercial, open-source, and government-facing software. The program intersects with federal compliance frameworks at multiple points. NIST's [Cybersecurity Framework \(CSF\)](#) maps vulnerability management to the "Identify" and "Protect" functions, and NIST SP 800-53 Revision 5 (control family RA — Risk Assessment) requires federal agencies to correlate findings against the CVE list as part of continuous monitoring programs. For



finance.yahoo.com

At Yahoo Finance, you get free stock quotes, up-to-date news, portfolio management resources,...

89
Domain
Authority ?
Provided by
MOZ

42.2M
Unique
Visits ?
Provided by
SimilarWeb

yahoo!finance Search for news, tickers or co... News Finance Sports More v Sign in

My Portfolio News Markets Research Community ... Network Try AlphaSpace Upgrade to Premium

US Markets S&P 500 7,408.31 +54.29 +0.74% Dow 30 52,105.96 +229.85 +0.44% Nasdaq 25,635.35 +337.73 +1.34% Russell 2000 2,977.21 -32.88 -1.09% VIX 18.35 -0.06 -0.33%

Quote Lookup

This is a paid press release. Contact the press release distributor directly with any inquiries.

businesswire

Jumpmind CISO Eric Zielinski to Introduce New Open-Source AI Interpretability Framework at FIRST Conference 2026

 Jumpmind

Business Wire
June 15, 2026 • 3 min read

The offering gives security teams a practical path to risk management and accountable AI

COLUMBUS, Ohio, June 15, 2026--(BUSINESS WIRE)-- Jumpmind Chief Information Security Officer Eric Zielinski will speak on AI interpretability risk management at the FIRST Annual Conference 2026 (FIRSTCON26) taking place in Denver this week.

During his talk, he will unveil CIRCUIT, a new open-source framework for AI interpretability risk management built

Jun 15, 2026 · ONLINE

News

Jumpmind CISO Eric Zielinski to Introduce New Open-Source A...

finance.yahoo.com/sectors/technology/ar...

Estimated Views

321K



HackerStorm.com

Global source for real-time CVE data, KEV alerts, and AI breach analysis. Get expert guidance on vulnerability remediation and threa...

19

Domain
Authority [?]

Provided by
MOZ

Feb 15, 2026 · ONLINE

Feature

59,000 CVEs in 2026: What the Record Forecast Means for...

hackerstorm.com/articles/our-blog/vulner...

Estimated Views

715

HACKERSTORM

HomeIntelligence ▾Search ▾Articles ▾About Us

Search ...

Hackerstorm Threat Intelligence - 15 February 2026
- Last Updated: 21 June 2026 - Hits: 4949

59,000 CVEs in 2026: What the Record Forecast Means for Vulnerability Management | Hackerstorm

Featured

GENEVA, Switzerland - February 16, 2026 - The Forum of Incident Response and Security Teams (FIRST) has released its 2026 Vulnerability Forecast, projecting a record-breaking 59,427 new CVEs this year. This unprecedented volume marks the first time the industry is expected to surpass the 50,000-vulnerability threshold, demanding a fundamental transition from manual patching to machine-speed, risk-based prioritization.

2026 CVE Volume Tracker

"Updated June 2026: As of mid-June 2026, NVD has published 34307+ CVEs year to date — tracking broadly in line with FIRST's 59,427 annual forecast. At current velocity, the daily publication rate averages 82 CVEs per day."

GENEVA, Switzerland - February 16, 2026 - The Forum of Incident Response and Security Teams (FIRST) has released its 2026 Vulnerability Forecast, projecting a record-breaking 59,427 new CVEs this year. This

Blog Categories

- Government & Regulatory Alerts (12)
- Operational Threat Intelligence & Lessons Learned (8)
- AI Threats & Fraud Intelligence (12)
- Vulnerability Intelligence (8)

Recent Posts

- 05 June 2026
Vulnerability Backlog: Why CVSS Prioritisation Is Broken and How to Fix It | Hackerstorm
- 27 May 2026
Identity as Initial Access: Credential Theft



World Bank Blogs

Stay up-to-date on the latest development trends, research and more through World Bank blogs.

92

Domain
Authority ?

Provided by
MOZ

375K

Unique
Visits ?

Provided by
SimilarWeb

🌐 ONLINE

Feature

Protecting Mozambique's digital future: Cyber...

blogs.worldbank.org/en/nasikiliza/protecti...

Estimated Views

788

WORLD BANK  **BLOGS**

HOME ALL BLOGS TOPICS CONTACT

WORLD BANK.ORG

WE LIVE

Q

Published on **Nasikiliza**

Protecting Mozambique's digital future: Cyber resilience for jobs, trust, and growth

ANNE-ELISABETH COSTAFROLAZ, GIACOMO ASSENZA & JACQUELINE PATEGUANA | MAY 20, 2026

This page in: English



Photo: John Hogg / World Bank

On a hot afternoon in 2018, hospitals, schools, hotels, and small businesses across Mozambique suddenly found themselves unable to process electronic payments. Patients could not pay doctor fees, parents could not settle school charges, motorists could not purchase fuel, and travelers both in-country and abroad were left unable to pay their bills. The cause was not a power outage nor maintenance, but a system-wide failure of the country's national payment system, **SIMORede**.

The blackout was triggered unexpectedly by a licensing dispute with the system's software provider. Although not malicious, the incident exposed a critical and often overlooked dimension of cybersecurity and digital resilience—the dependence of essential services on external vendors and contractual



New Era

51
Domain
Authority ?
Provided by
MOZ

32.2K
Unique
Visits ?
Provided by
SimilarWeb

Jun 24, 2026 · ONLINE

News

Namibia shares cybersecurity experience at global...

neweralive.na/namibia-shares-cybersecur...

Estimated Views

444

Engagements

1

NEWS FOCUS FEATURED PHOTO OF THE WEEK GALLERY PODCASTS EPAPER ELECTIONS Q

BUSINESS

Namibia shares cybersecurity experience at global conference

2026-06-24 | BY STAFF REPORTER

SHARE THIS POST?

RECENT POSTS

- Iran FM warns Hormuz routes will 'increase tensions'
- Eeproyeka dokutunga oupale otadi ende nawa mOshana
- Unam na Mighty Gunners va findana po ekopi lo NFA ... Alweendo na Amutenya ovo oবাদani dingi
- Oilongo ya Africa omuwai kedingonoko 32 kekopi lounyuni
- Unam a ungeneka oshivilo shopamufyuululwakalo

300 x 500

Advertise Here

300 x 500



Windhoek Observer – Democracy in the mirror

42

Domain
Authority ?

Provided by
MOZ

18.3K

Unique
Visits ?

Provided by
SimilarWeb

Jun 23, 2026 · ONLINE

News

Namibia represented at global cybersecurity...

observer24.com.na/namibia-represented-...

Estimated Views

2.68K

Engagements

1

Tuesday, June 23 15:41:45

WINDHOEK OBSERVER

Home > Observer Money > Namibia represented at global cybersecurity conference

OBSERVER MONEY

NAMIBIA REPRESENTED AT GLOBAL CYBERSECURITY CONFERENCE

6 hours ago 113 2 Mins Read



WINDHOEK OBSERVER

Staff Writer

WINDHOEK OBSERVER

BE SEEN

ADVERTISE WITH WINDHOEK OBSERVER

Web, social and WhatsApp reach for brands that want results.

WEB. SOCIAL. RESULTS.

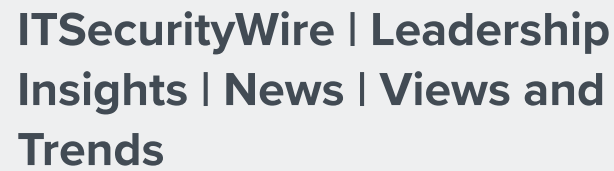
ENQUIRE TODAY

www.observer24.com.na

sales@observer.com.na

JOIN OUR CHANNEL

BE SEEN. BE HEARD. GET A WINDHOEK OBSERVER



31
Domain
Authority 
Provided by
MOZ

 ONLINE

itsecuritywire.com/interview/unifying-cyber-security

736





PressReader.com - Digital Newspaper & Magazine Subscriptions

Digital newsstand featuring 7000+ of the world's most popular newspapers & magazines. Enjoy unlimited reading on up to 5 devices with 7-day free trial.

Jun 24, 2026 · ONLINE

PressReader.com - Digital Newspaper & Magazine...

pressreader.com/namibia/new-era/20260...

The screenshot displays the PressReader.com homepage. At the top, there's a navigation bar with 'CATALOG', 'FOR YOU' (selected), and 'MORE'. The 'pressreader' logo is in the center, followed by 'Gift Cards', a search icon, and 'Sign in' and 'Sign up' buttons. Below the navigation bar, the 'Region & Language' is set to 'United States (English)'. The left sidebar contains 'Sections' (Top Stories, Recommended, Politics, Business, Tech, Health, Sports, Science, Arts, Entertainment) and 'Publications' (Coronavirus (COVID-19), Politics, Crime, U.S. News, Business). The main content area features a 'Top Stories' section with four articles: 1. 'Namibia shares cybersecurity experience at global confer-...' from 'new era' (24 Jun 2026). 2. 'US and Iranian strikes threaten fragile peace' from 'The Guardian' (29 Jun 2026). 3. 'Venezuela quake death toll rises to 1,450 as aftershocks hamper rescues' from 'Miami Herald' (29 Jun 2026). 4. 'Russia hit hard by Ukr.' from 'NEW YORK POST' (29 Jun 2026). Each article includes a thumbnail image, headline, brief description, category tags, and a 'READ THIS ARTICLE' button.

A

Penetration Testing Authority

Penetrationtestingauthority is a structured reference and directory covering the penetration testing service sector in t

2

Domain
Authority [?]

Provided by
MOZ

Mar 12, 2026 ·  ONLINE

Feature

Penetration Testing Reporting Standards | Penetration Testing...

penetrationtestingauthority.com/penetrati...

Filter pages...

← National Cyber Authority

► OVERVIEW

► CAREERS & CERTIFICATIONS

► COMPLIANCE & REGULATIONS

► HIRING & PROCUREMENT

► INDUSTRY APPLICATIONS

► LEGAL & AUTHORIZATION

► TECHNIQUES & TOOLS

► TESTING TYPES & APPROACHES

► CALCULATORS

► RELATED SITES

FAQ

Get Help

Editorial Review & Corrections

PENETRATION TESTING AUTHORITY

AUTHORITY NETWORK AMERICA

ANA > Professional Services Authority > National Cyber > Penetration Testing Authority

Penetration Testing Reporting Standards

Penetration testing reporting standards define the structure, content requirements, and delivery expectations that govern how findings from authorized security assessments are documented and communicated. These standards operate at the intersection of methodology, compliance, and professional accountability — shaping how vulnerability data is classified, prioritized, and acted upon across regulated industries in the United States. Reporting quality directly determines whether an engagement produces defensible, audit-ready evidence or a document that satisfies neither security teams nor compliance auditors.

Definition and scope

A penetration testing report is the primary deliverable of any authorized security engagement. Unlike raw scanner output or informal findings logs, a formal report must demonstrate that identified vulnerabilities were actively exploited or proven exploitable, document the chain of evidence supporting each finding, and map results to a recognized risk classification framework.

No single federal statute mandates a universal penetration testing report format. Instead, reporting standards emerge from a cluster of regulatory frameworks and professional methodology documents. [NIST SP 800-115, Technical Guide to Information Security Testing and Assessment](#) establishes baseline documentation expectations for federal information systems, including the requirement that assessment reports include objectives, scope, approach, findings, and recommendations. PCI DSS v4.0, Requirement 11.4, administered by the [PCI Security Standards Council](#), requires that penetration testing results and remediation activities be retained for at least 12 months. FedRAMP, operated by the [General Services Administration](#), mandates penetration test reports as part of the security authorization package for cloud service providers seeking federal agency authorization.

The scope of reporting standards encompasses 4 primary domains: finding classification and severity scoring, evidence documentation requirements, remediation guidance structure, and executive-level risk communication. Each domain carries distinct requirements depending on the regulatory context governing the assessed organization.



Windhoek Express

Windhoek Express home5

30

Domain
Authority ?

Provided by
MOZ

1.47K

Unique
Visits ?

Provided by
SimilarWeb

Jun 23, 2026 · ONLINE

News

NAM-CSIRT at Denver global cyber security conference

we.com.na/technology-we/nam-csirt-at-d...

Estimated Views

585

EXAM RESULTS

RETAIL SPECIALS

WHATSAPP

LOGIN

Monday 29 June 2026, 15:41:52

f

yt

in

WE

Windhoek Express

DIGITAL EDITION

SERVICES

PUBLICATIONS

LOCAL NEWS

ENTERTAINMENT

EDUCATION

EVENTS

SUBSCRIPTION

COMPETITIONS

CLASSIFIEDS

HOME / TECHNOLOGY / NAM-CSIRT AT DENVER GLOBAL CYBER SECURITY CONFERENCE

ADVERTISEMENTS

f

x

in

TECHNOLOGY

NAM-CSIRT AT DENVER GLOBAL CYBER SECURITY CONFERENCE

-

-

Staff reporter

6 DAYS AGO - 2026-06-23 00:05:00

The Namibia Cyber Security Incident Response Team (NAM-CSIRT) represented Namibia at the 38th Annual Forum of Incident Response and Security Teams (FIRST) Conference, held from 14 to 19 June 2026 in Denver, Colorado, USA.

Convened under the theme "Peak Defense: Building Adaptive Systems for Modern Threats," the conference brought together the global incident response and cybersecurity community to advance collaboration, resilience, and preparedness against evolving cyber threats. NAM-CSIRT was admitted as a FIRST member in December 2025 and is also participating in the Suguru Yamaguchi Fellowship Programme.

The conference provided a platform for Computer Security Incident Response Teams (CSIRTs), policymakers, technical experts, and industry partners to strengthen global cyber resilience. Through technical sessions, workshops, and high-level engagements, participants exchanged insights on emerging cyber threats, incident response, threat intelligence, digital resilience, and international cooperation.

Ahead of the main conference, the NAM-CSIRT delegation participated in the NAT-CSIRT Meeting, held on 12 and 13 June 2026. The meeting served as a dedicated forum for National CSIRTs to share information, tools, techniques, operational experiences, and strategies for addressing cybersecurity challenges at national and economic levels.

Cornelia Shipindo, Acting Executive: NAM-CSIRT, served on the NAT-CSIRT 2026 Programme Committee, contributing to the coordination of activities and key topic presentations.

Local

Windhoek

Technology WE

NAM CSIRT

NMH012596_4_15389

RELATED POST



bjCSIRT

15
Domain
Authority ?
Provided by
MOZ

209
Unique
Visits ?
Provided by
SimilarWeb

🌐 ONLINE

News

Publications – bjCSIRT

csirt.bj/category/publications

Estimated Views

122

**bjCSIRT**
RÉPUBLIQUE DU BÉNIN

Accueil | Alertes | Publications | Déclarer un incident 🔍

Participation du bjCSIRT et du CNIN au Cyber Games 2026

🕒 26 mai 2026



Actualités Récentes

- Multiples vulnérabilités affectant des extensions WordPress 29 juin 2026
- Multiples vulnérabilités affectant NGINX 19 juin 2026
- Contournement d'authentification affectant Palo Alto Networks PAN-OS 19 juin 2026
- Campagne massive de compromission des équipements FortiGate 18 juin 2026
- Exécution de code à distance affectant Joomla Content Editor (JCE) 18 juin 2026
- Exécution de code à distance affectant Netlogon 18 juin 2026
- Exécution de code à distance affectant FortiSandbox 18 juin 2026



脆弱性診断（セキュリティ診断）のGMOサイバーセキュリティ byイエラエ

脆弱性診断、ペネトレーションテスト、SOCなどのセキュリティ対策なら診断実績1.2万件を超える...

38
Domain
Authority [?]
Provided by
MOZ

29.1K
Unique
Visits [?]
Provided by
SimilarWeb

Jun 01, 2026 · ONLINE

News

「FIRST Conference 2026」に取締役CGO林彦博と執行...

gmo-cybersecurity.com/news/20260601

Estimated Views

5.63K

ネットのセキュリティも GMO 無料診断 >

GMO大会議 >

おかげさまで 30.3連勝 GMO

GMO CYBER SECURITY IERAE

TOP > ニュース > お知らせ > 「FIRST Conference 2026」に取締役 CGO林彦博と執行役員の伊藤公祐が登壇します

「FIRST Conference 2026」に取締役 CGO林彦博と執行役員の伊藤公祐が登壇します

2026.06.01 [お知らせ](#)

世界最大級のインシデントレスポンス／セキュリティコミュニティである FIRST（Forum of Incident Response and Security Teams）が主催する年次カンファレンス「FIRST Conference 2026」において、取締役 CGO林彦博（りん ひこひろ）と執行役員の伊藤公祐がスピーカーとして登壇します。

「FIRST Conference」は、世界中の CSIRT、PSIRT、セキュリティ研究者、政府機関、企業の専門家が集まり、最新の脅威動向、インシデントレスポンス、脆弱性対応、AIセキュリティなど幅広いテーマを議論する国際会議です。

2026 年は 6 月 14 日～19 日に米国コロラド州デンバーのシェラトン・デンバー・ダウンタウン・ホテルにて開催され、基調講演、技術セッション、パネルディスカッション、Lightning Talks など多彩なプログラムが予定されています。

【登壇概要】

タイトル：PSIRT 2.0 in Action: Implementing Agentic AI Architecture for Autonomous Operations(PSIRT 2.0の実践：自律運用のためのエージェント型AIアーキテクチャの実装)

日時（現地時間）：2026年6月18日 10:55～11:30

トーク概要：PSIRT 2.0が掲げる「AI支援によるエコシステム連携」は、年間4万件以上のCVE、複雑なサプライチェーン、EU CRAやNIS2などの規制強化に直面する製品セキュリティチームの維持危機を救うと期待されています。しかし、完全なAI自動化では判断の正確性が担保できず、人手だけでは規模拡大に対応できないという課題が生じています。

本セッションはFIRST年次カンファレンスにおける3部作の完結編であり、自動化と人間の判断を両



TAdviser.ru

Government. Business. Technology

43

Domain
Authority ?

Provided by
MOZ

74.2K

Unique
Visits ?

Provided by
SimilarWeb

Aug 03, 2025 · ONLINE

Roundup

Ransomware, spyware and keyloggers. How...

tadviser.com/index.php/Article:Cyber_att...

Estimated Views

9.77K

RSS

TADVISER
Government. Business. IT

Model Studio CS:
How to use BIM to give
new impetus to the
development of the
fuel and energy
complex

Information modeling
technologies:
a confident course
for import
substitution

Search

News

2026/06/11 11:10:41

Cyber attacks on critical information infrastructure

Content

Collapse

Security of critical information infrastructure of the Russian Federation

2026

Ransomware, spyware and keyloggers. How hackers attack APCS in Russia

Detection of wiretapping of smartphones of Russian officials using the technologies of the American Cloudflare and Fastly

Hackers hacked IT systems of water treatment plants in 5 cities in Poland and left people without water

The share of cyber attacks on critical infrastructure in Russia in the first quarter reached a record 77%

Hackers infiltrated the FBI's IT system for surveillance and telephone wiretapping. The Bureau acknowledged this

Romania's national oil company, Conpet, has been attacked by hackers. Servers shut down, passport scans and financial documents stolen and uploaded online

Hackers hacked into Poland's power grid and permanently destroyed key equipment

Spanish energy firm Endesa's servers hacked

Hackers hacked into servers of Spain's largest airline Iberia and stole 77GB of data, including aircraft damage schemes

2025

Company: European Space Agency (ESA)

Hackers shut down US-wide emergency alert system

The infrastructure of the company serving six marine terminals in Russia was subjected to a large-scale DDoS attack

'Leave the station immediately': Hackers break into Los Angeles' IT transport infrastructure and bring threats to subway screens

The airline "KrasAvia" was attacked by hackers. The site has been down for several days

Linux ship management systems have been hacked in Iran. Dozens of tankers idle

Hackers attack US industrials using fake nondisclosure agreements

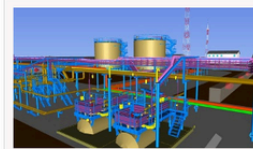
Hackers stopped the work of hydroelectric power plants in Poland and told how they did it

Cyber espionage group PhantomCore attacked objects of Russian critical infrastructure

The Russian Datahouse data center network was attacked by hackers. The main trunk



How to create a "smart plant": Key characteristics of a modern digital enterprise
17500



Model Studio CS: How to use BIM to give new impetus to the development of the fuel and energy complex
20500



Ransomware Authority

The ransomware service sector spans incident response firms, forensic investigators, legal couns...

3
Domain
Authority ?
Provided by
MOZ

282
Unique
Visits ?
Provided by
SimilarWeb

Filter pages...

← National Cyber Authority

OVERVIEW

ATTACK MECHANICS

DETECTION & PREVENTION

INCIDENT RESPONSE & RECOVERY

LEGAL & COMPLIANCE

PAYMENTS & NEGOTIATION

RANSOMWARE VARIANTS & ACTORS

SECTOR THREATS

STATISTICS & COSTS

CALCULATORS

RELATED SITES

FAQ

Get Help

Editorial Review & Corrections

RANSOMWARE AUTHORITY

AUTHORITY NETWORK AMERICA

ANA > Professional Services Authority > National Cyber Authority > Ransomware Authority > Vulnerability Management to Reduce Ransomware Exposure

Vulnerability Management to Reduce Ransomware Exposure

Vulnerability management is a structured security discipline focused on identifying, prioritizing, and remediating weaknesses in systems, software, and configurations before threat actors can exploit them. In the ransomware context, unpatched vulnerabilities represent one of the primary initial access vectors used by ransomware operators — making vulnerability management a foundational layer of ransomware exposure reduction. This page describes the service sector, professional frameworks, regulatory obligations, and decision boundaries that define vulnerability management practice as applied to ransomware risk, drawing on standards from NIST, CISA, and sector-specific regulatory bodies.

Definition and scope

Vulnerability management is defined by [NIST SP 800-40 Rev. 4](#) as a planned, systematic process for identifying, acquiring, installing, and verifying patches and mitigations for software and firmware vulnerabilities across an enterprise. In the ransomware threat landscape, this scope extends to configuration weaknesses, exposed remote access services, and unsupported software that ransomware operators routinely enumerate using publicly available exploit code.

[CISA's Known Exploited Vulnerabilities \(KEV\) Catalog](#) — a binding directive for federal civilian executive branch agencies under Binding Operational Directive 22-01 — catalogs vulnerabilities that have been actively exploited in the wild. As of 2023, CISA had added over 1,000 entries to the KEV catalog, a substantial portion of which correspond to vulnerabilities used in ransomware campaigns. Ransomware groups including LockBit and ALPHV/BlackCat have documented histories of exploiting CVEs within days of public disclosure, compressing the remediation window organizations have available.

The scope of vulnerability management in a ransomware-reduction context spans four asset classes:

- **Network perimeter assets** — VPN appliances, firewalls, and remote desktop gateways that provide initial access

Mar 12, 2026 · ONLINE

Feature

Vulnerability Management to Reduce Ransomwar...

ransomwareauthority.com/vulnerability-m...

Estimated Views

217



Help Net Security

Cybersecurity news with a focus on enterprise security. Discover what matters in the world of...

76

Domain
Authority ?

Provided by
MOZ

209K

Unique
Visits ?

Provided by
SimilarWeb

Jun 21, 2026 · ONLINE

Roundup

Week in review: 74k Fortinet firewall credentials stolen,...

helpnetsecurity.com/2026/06/21/week-in-...

Help Net Security newsletters: Daily and weekly news, cybersecurity jobs, open source projects, breaking news – [subscribe here!](#)

HELP NET SECURITY
News Features CISO AI Videos Product showcase Industry news Reviews Whitepapers Events Newsletters

Hidden identities create hidden risk.
How do you achieve full visibility? [GET THE CISO GUIDE](#)

Week in review: 74k Fortinet firewall credentials stolen, Splunk Enterprise RCE under active attack
Here's an overview of some of last week's most interesting news, articles, interviews and videos:

CYBERSECURITY WEEK IN REVIEW
A hardware neural network backdoor that hides in plain sight
Deep learning systems on edge devices often rely on third-party-designed FPGAs and ASICs for performance and efficiency, creating supply chain risks. Researchers from the University of Tennessee and the University of Florida developed HAMLOCK, a backdoor attack that splits malicious functionality between hardware and software, making detection more difficult.
Onspring CISO on where automated GRC systems fall short
In this interview with Help Net Security, Nichole Windholz, CISO at Onspring, talks about the limits of automated GRC systems and continuous control monitoring. She explains why color-coded dashboards can hide nuance, how teams can check the data feeding their tools, and which risks resist measurement, such as insider behavior and vendor concentration.

Featured news
DarkMoon: Open-source AI pentesting platform
Synology issues critical fix for MailPlus Server vulnerabilities
Mystery hackers use novel SharkLoader dropper against governments, software devs

Resources
Download: Secure Foundations for AI Workloads on AWS
Download: Automating Pentest Delivery Guide
CIS Benchmarks March 2026 Update

Estimated Views

1.28K

Engagements

7



HackerStorm.com

Global source for real-time CVE data, KEV alerts, and AI breach analysis. Get expert guidance on vulnerability remediation and threa...

19

Domain
Authority [?]

Provided by
MOZ

Feb 15, 2026 · ONLINE

News

Six Microsoft Zero-Days Under Active Exploitation - Patch...

hackerstorm.com/articles/our-blog/operat...

Estimated Views

715

HACKERSTORM Home Intelligence ▾ Search ▾ Articles ▾ About Us CVE Id ...

Blog Categories

- Government & Regulatory Alerts (12)
- Operational Threat Intelligence & Lessons Learned (8)
- AI Threats & Fraud Intelligence (12)
- Vulnerability Intelligence (8)

Recent Posts

-  05 June 2026
Vulnerability Backlog: Why CVSS Prioritisation Is Broken and How to Fix It | Hackerstorm
-  27 May 2026
Identity as Initial Access: Credential Theft, ...



Hackerstorm Threat Intelligence - 15 February 2026
- Last Updated: 28 June 2026

Six Microsoft Zero-Days Under Active Exploitation - Patch Before March 3 | HackerStorm

WASHINGTON, D.C. - February 16, 2026 - The Cybersecurity and Infrastructure Security Agency (CISA) has issued a mandatory federal directive requiring the remediation of six Microsoft zero-day vulnerabilities by March 3. Linked to active exploitation by nation-state actors including Salt Typhoon, these flaws represent a critical escalation in the 2026 vulnerability landscape.

WASHINGTON, D.C. - February 16, 2026 - The Cybersecurity and Infrastructure Security Agency (CISA) has issued a mandatory federal



株式会社ラック

株式会社ラックは、先進のセキュリティ対策技術を核としたITトータルソリューションで、お客様...

51

Domain
Authority ?

Provided by
MOZ

35.1K

Unique
Visits ?

Provided by
SimilarWeb

Jun 18, 2026 · ONLINE

News

38th Annual FIRST Conference | イベント・セミナー | LAC...

lac.co.jp/lacwatch/event/20260618_004...

Estimated Views

739

LAC WATCH | セキュリティとITの最新情報

LAC

注意喚起

テクニカルレポート

サービス・製品

イベント・セミナー

導入事例

ラックビブル

広報情報

お知らせ

タグ +

ライター

メールマガジン
サイバーセキュリティや
ラックに関する情報をお届けします。
登録する

f

X

o

イベント・セミナー

38th Annual FIRST Conference

オンサイト アメリカ

開催日: 2026年6月14日(日) ~ 19日(金)

Twitter

f

Bl

note

メールマガジン登録する

第38回 FIRST 年次カンファレンス (38th Annual FIRST Conference、FIRST主催) は、2026年6月14日(日) ~ 19日(金) (現地時間)、米国コロラド州デンバーで開催されます。

ラック社員が登壇し、講演します。皆様のご参加をお待ちしています。

プログラム

6月18日(木) | 15:05 - 15:40 (現地時間)

適応型回避に対抗するプロアクティブEDR: 自己改変型エージェントマルウェアへの防御戦略
(原題: Proactive EDR Against Adaptive Evasion: Countering Self-Modifying Agentic Malware)

G

DJ-CERT - Centre gouvernementale de veille, d'alertes et de réponses aux attaques informatiques

Baako - Responsive HTMaL5 CSS3 Template

40

Domain

Authority ?

Provided by

MOZ

🌐 ONLINE

News

DJ-CERT - Centre gouvernementale de veille, d'alertes et d...

cert.gouv.dj/Article/getArticleDetails/20



FORMATION AVANCÉE EN INVESTIGATION NUMÉRIQUE ET ANALYSE FORENSIQUE WINDOWS & LINUX ORGANISÉE PAR L'ANC EN COLLABORATION AVEC FIRST ET LE MDENI

FORMATION AVANCÉE EN INVESTIGATION
NUMÉRIQUE ET ANALYSE FORENSIQUE
WINDOWS & LINUX ORGANISÉE PAR L'ANC EN
COLLABORATION AVEC **FIRST** ET LE **MDENI**

18.05.26 - 20.05.26

HOTEL AYLA



Djibouti, du 18 au 20 mai 2026 – L'Autorité Nationale de Cybersécurité (ANC), à travers le DJ-CERT, a organisé une « Formation avancée en Investigation Numérique et Analyse Forensique Windows & Linux » en collaboration avec le Forum of Incident Response and Security Teams (FIRST) et le Ministère de l'Économie Numérique et de l'Innovation (MDENI). Cette session de formation, répartie sur trois jours, a réuni plusieurs participants issus de l'administration publique et des opérateurs d'importance vitale.

Cette initiative s'inscrit dans les efforts continus de renforcement des capacités nationales en matière de cybersécurité et de développement des compétences techniques liées à la détection, l'analyse et l'investigation des incidents de sécurité informatique. Elle fait également suite à la participation du DJ-CERT au Symposium FIRST & AfricaCERT 2025, durant lequel une formation spécialisée sur l'analyse forensique des ransomwares avait été dispensée au profit de CERT africains et d'experts internationaux.

La formation avait pour principaux objectifs de renforcer les capacités d'analyse des événements de sécurité et d'améliorer la détection des activités suspectes, de développer les compétences en gestion et en priorisation des incidents de sécurité, de consolider les connaissances en investigation numérique ainsi que d'approfondir les



Revista SIC – Revista de Ciberseguridad, Seguridad de la Información y Privacidad

Revista de Ciberseguridad, Seguridad de la información y Privacidad

32
Domain Authority 
Provided by MOZ

2.36K
Unique Visits 
Provided by SimilarWeb

Jun 01, 2026 ·  ONLINE

Feature

Los CSIRT con sede en España en los foros de referencia

revistasic.es/agora-sic/los-csirts-espanole...

Estimated Views

752

Engagements

15





🕒 1 junio, 2026

Volver a SIC | Volver a Ágora SIC

Los CSIRT con sede en España en los foros de referencia

Desde hace más de tres décadas, los equipos de respuesta a incidentes de ciberseguridad, conocidos como CERT / CSIRT, han ido ganando en experiencia y madurez y hoy se consideran esenciales -tanto para entidades públicas como privadas- al objeto de hacer frente a los ciberataques y elevar el nivel de resiliencia.

Para acreditar su desempeño inicial hay diferentes entidades que los reconocen y que, además, sirven como foro de intercambio de información de estos equipos.

(Ver SIC 142, páginas 81-98, <https://revistasic.es/sic142/revistasic142.pdf>).

Entre las organizaciones que los agrupan destaca la universidad Carnegie Mellon, creadora de la marca 'CERT' -aunque desde mediados de 2020 ya no otorga la licencia de uso fuera de EE.UU. (<https://www.sei.cmu.edu/our-work/cybersecurity-center-development/authorized-users/>), el FIRST (Forum of Incident Response and Security Teams), el Trusted Introducer (TF-CSIRT) y la Agencia de Ciberseguridad de la UE (Enisa), que ofrece un mapa con todos los presentes en el Viejo Continente. En España, desde 2018, impulsado por el CCN, está muy activo el foro CSIRT.es.

SIC pone a disposición de los lectores un cuadro con actualizaciones periódicas (la última a fecha de 1-6-2026) de los equipos de CERT / CSIRT que, con sede en España, son reconocidos por los diferentes foros o están en proceso de serlo.

NOMBRE(S)	ENISA	FIRST	TRUSTED INTRODUCER	CSIRT.es	CERT (Carnegie Mellon) Solo hasta 4/2021
- Accenture CSIRT Iberia				✓	
- ACN_IBE_CSIRT	✓	✓	Candidato a re-registro		
- ACN IBE CSIRT	✓			✓	
- Innotec Security CSIRT					



CirebonKota-CSIRT

36
Domain
Authority ?
Provided by
MOZ

342
Unique
Visits ?
Provided by
SimilarWeb

ONLINE

Feature

CirebonKota-CSIRT

csirt.cirebonkota.go.id/posts/mengenal-c...

Estimated Views

80



Beranda Profil Artikel RFC2350 Layanan Panduan Kontak

Mengenal CVE: Kunci Utama Menjaga Keamanan Sistem Informasi

Published By Sultan in Literasi Digital



Mengenal CVE Kunci Utama Menjaga Keamanan Sistem Informasi

Pernahkah Anda mendengar istilah seperti "Ditemukan celah keamanan kritis CVE 2026 0628 pada browser Anda"? Bagi masyarakat awam deretan angka dan huruf tersebut mungkin terlihat seperti kode acak yang rumit. Namun di dunia keamanan siber kode inilah yang menyelamatkan jutaan sistem dari serangan peretas setiap harinya. Mari kita bedah apa itu CVE dan mengapa keberadaannya sangat penting bagi keamanan data kita **Apa Itu CVE:**

CVE adalah singkatan dari **Common Vulnerabilities and Exposures**. Secara sederhana CVE adalah sebuah kamus atau daftar publikasi referensi global yang mendata seluruh celah keamanan vulnerability yang ditemukan pada perangkat lunak software maupun perangkat keras hardware

Kamus global ini dikelola secara internasional oleh MITRE Corporation sebuah organisasi nirlaba asal Amerika Serikat yang didanai oleh pemerintah federal. Setiap kali ada peneliti keamanan atau vendor yang menemukan celah baru celah tersebut akan dilaporkan diverifikasi dan diberi satu nomor identitas unik standar yang disebut CVE ID.



Red Hat - We make open source technologies for the enterprise

Red Hat is the world's leading provider of open source solutions, using a community-powered...

92
Domain
Authority [?]
Provided by
MOZ

1.46M
Unique
Visits [?]
Provided by
SimilarWeb



Red Hat Blog

Cookie Preferences and Opt-Out Rights Your Choices About Cookies on this Site

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Accept default will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

Required Cookies only will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

Clearing your browser cookies may delete your cookie preferences. If you re-visit this site after clearing browser cookies, you will need to reset your preferences at that time. If you have set your browser's global privacy settings, then we recognize the global privacy settings from your browser.

Accept default

Required Cookies only

[Cookie Preferences and Opt-Out Rights](#) | [Privacy Statement](#)

Blog post

Supercharge RHEL troubleshooting with agentic AI: Introducing goose

Blog post

Distributed AI inference: What telecom service provider leaders should know

Original podcast

AI cod
develc
adopt
compr
operational compliance.

AI has changed the economics of code production

Whether you're developing software in a proprietary enterprise or open source environment, you've witnessed a fundamental shift over the past year. Your developers are using AI coding assistants (GitHub Copilot, Cursor, Claude Code, ChatGPT Codex, etc.) to accelerate development. Productivity gains are real—features can ship faster and developers can spend more time on

Jun 22, 2026 · ONLINE

Feature

The AI code paradox: Moving fast without breaking security

redhat.com/en/blog/ai-code-paradox-mov...

Estimated Views

4.07K

Engagements

2



INCYBER NEWS

Le média de la confiance numérique

42

Domain
Authority ?

Provided by
MOZ

11.3K

Unique
Visits ?

Provided by
SimilarWeb

Jun 25, 2026 · ONLINE

Feature

La gestion des vulnérabilités dans la tourmente Mythos -...

incyber.org/article/la-gestion-des-vulnera...

Estimated Views

1.48K





Resilient Cyber | Chris Hughes | Substack

Resilient Cyber distills the week's most important news, research, and writing across AppSec, AI...

30
Domain
Authority [?]
Provided by
MOZ

3K
Unique
Visits [?]
Provided by
SimilarWeb

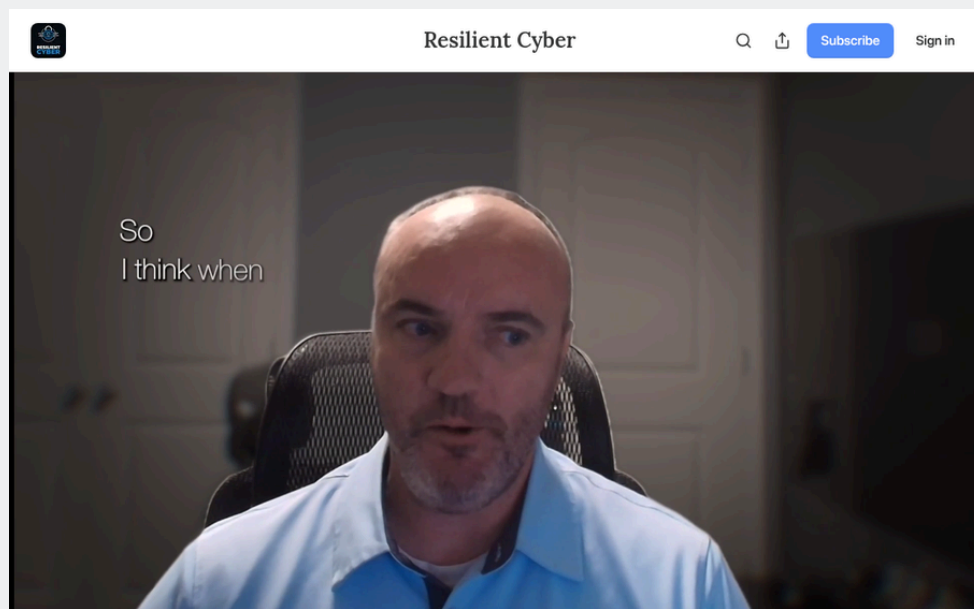
Jun 28, 2026

ONLINE

Interview

Why 70,000 CVE's is Less Scary Than It Sounds

resilientcyber.io/p/why-70000-cves-is-less-scary-than-it-sounds



Why 70,000 CVE's is Less Scary Than It Sounds

The count is exploding, the exploitable risk is flat, and Jerry Gamblin explains why



CHRIS HUGHES
JUN 28, 2026



5



2



1

Share

Every few weeks another headline warns that vulnerability disclosures are setting records, and 2026 is now on pace for nearly 70,000 CVEs. Jerry Gamblin helped build the forecast behind that number, and his takeaway is not the one you would expect. The count is surging, but the risk that actually matters has barely moved.

Why this conversation matters

Jerry runs RogoLabs, built CVE.ICU, and co-authored the FIRST mid-year forecast,



Resilient Cyber

Type your email...

Subscribe

Authors



Chris Hughes

Recent Posts



You Don't Need A Frontier Model to Find Zero Days

JUN 22 • CHRIS HUGHES



The Bottleneck Was Never End of the Road

Estimated Views

1K

Engagements

1

securityonline.info/zkteco-cctv-camera-vu...



@IT

プロフェッショナルなIT技術者・管理者のためのコンテンツとコミュニティ満載の問題解決サイト。...

90

Domain Authority ?

Provided by MOZ

1.42M

Unique Visits ?

Provided by SimilarWeb

Jun 17, 2026 · ONLINE

News

AIが脆弱性を掘り起こし過ぎる時代へ FIRSTがCVE予測を6...

atmarkit.itmedia.co.jp/ait/articles/2606/18...

Estimated Views

3.3K

Engagements

6

35th ANNIVERSARY

@IT

連載一覧

連載まとめ読み@IT eBook

記事ランキング

@IT Special

セミナー

ホワイトペーパー

クラウド

AI IoT

アジャイル/DevOps

セキュリティ

キャリア&スキル

Windows

初・中級者向けAI

その他

AIを作り動かし守り生かす

ローコード/ノーコード

クラウドネイティブ

Microsoft&Windows

その他の特集

マイページ

@IT > セキュリティ > Security & Trust > AIが脆弱性を掘り起こし過ぎる時代へ FIRSTがCVE予...

脆弱性増での新課題とは？

AIが脆弱性を掘り起こし過ぎる時代へ FIRSTがCVE予測を6万6000件に上方修正

脆弱性の急増は、防御側にとって本当に悪いニュースなのか。FIRSTの最新予測によると、AIの進化によって脆弱性の発見件数は想定を大きく上回るペースで増加している。一方で、企業が優先対応すべき脆弱性の数は大きく変わっていないという。

© 2026年06月18日 07時30分 公開

【@IT】

印刷

見る

Share

BI

この記事は会員限定です。会員登録(無料)すると全てご覧いただけます。

FIRST(Forum of Incident Response and Security Teams)は2026年6月15日(現地時間)、脆弱(ぜいじゃく)性予測レポートの年次更新版「The 2026 Vulnerability Forecast Update: Navigating the AI Epoch」を公表した。AIによる脆弱性発見能力の急速な向上などを受けて、2026年の脆弱性情報データベース(CVE)の登録件数予測を約6万6000件に引き上げた。

一方、企業が優先的に対処すべき脆弱性の規模は大きく変わっていないとも指摘する。脆弱性管理の課題は「脆弱性が増えること」よりも、「膨大な情報の中から本当に対応すべき脆弱性を選び出すこと」に移りつつあるという。

AIが押し上げるCVE件数「脆弱性の洪水」は始まったのか？

今回のレポートは、FIRSTが年初に公表した2026年予測を実績データに基づいて見直したものだ。

FIRSTによると、2026年上半年までに確認された脆弱性情報の累積件数は当初予測を46.3%上回り、超過分は6420件に達した。この結果を受けて、年間予測値を約6万6000件へ引き上げた。

CVE-Explosion: 66.000 Sicherheitslücken bi...

ad-hoc-news.de/wissenschaft/cve-explosi...

Estimated Views

14.1K

BLOGS | BORSENLEXIKON | RSS | WATCHLIST

AD HOC NEWS
Finanzzeitung für Deutschland

Suche in News ... **News Suche**

NEWS AKTIENKURSE BÖRSE WIRTSCHAFT POLITIK SPORT UNTERHALTUNG **WISSENSCHAFT** AUSLAND POLIZEI INTERNATIONAL SONSTIGE

Sie befinden sich hier: Startseite > Wissenschaft > CVE-Explosion: 66.000 Sicherheitslücken bis Ende 2026 ...

CVE-Explosion, Sicherheitslücken

CVE-Explosion: 66.000 Sicherheitslücken bis Ende 2026 erwartet

15.06.2026 - 16:25:02 | boerse-global.de

AV-Comparatives zeichnet sieben Sicherheitslösungen mit der Höchstnote aus. Parallel warnt der Test vor einem neuen 3D-Asset-Wurm und steigenden Sicherheitslücken.



CVE-Explosion - A stylized, glowing padlock icon over an abstract digital landscape of code and data streams, representing cybersecurity.
15.06.2026 - Bild: über boerse-global.de

Die unabhängige Prüforganisation AV-Comparatives hat 20 Sicherheitslösungen getestet – sieben erreichen die höchste Stufe.

Wien/Innsbruck – AV-Comparatives veröffentlichte heute die Ergebnisse seines aktuellen „Real-World Protection Tests“ für den Zeitraum Februar bis Mai 2026. Die sieben Testsieger mit der Bestnote **ADVANCED+** heißen: **Avast, AVG, Bitdefender, Kaspersky, Microsoft, Norton und TotalAV**. Der