# Common Vulnerability Scoring System version 4.0

# Examples

## Document Version: 1.4

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of four metric groups: Base, Threat, Environmental, and Supplemental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Threat group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. Base metric values are combined with default values that assume the highest severity for Threat and Environmental metrics to produce a score ranging from 0 to 10. To further refine a resulting severity score, Threat and Environmental metrics can then be amended based on applicable threat intelligence and environmental considerations. Supplemental metrics do not modify the final score, and are used as additional insight into the characteristics of a vulnerability. A CVSS vector string consists of a compressed textual representation of the values used to derive the score. This document provides the official specification for CVSS version 4.0.

# Contents

## Resources & Links

Below are useful references to additional CVSS v4.0 documents.

| Resource | Location |
|---|---|
| Specification Document | Includes metric descriptions, formulas, and vector strings. Available at https://www.first.org/cvss/v4.0/specification-document |
| User Guide | Includes further discussion of CVSS v4.0, a scoring rubric, and a glossary. Available at https://www.first.org/cvss/v4.0/user-guide |
| Examples Document | Includes examples of CVSS v4.0 scoring in practice. Available at https://www.first.org/cvss/v4.0/examples |
| CVSS v4.0 Calculator | Reference implementation of the CVSS v4.0 equations, available at https://www.first.org/cvss/calculator/4.0 |
| JSON & XML Data Representations | Schema definition available at https://www.first.org/cvss/data-representations |
| CVSS v4.0 Main Page | Main page for all other CVSS resources: https://www.first.org/cvss/v4-0/ |

## Introduction

This document demonstrates how to apply the CVSS version 4.0 standard to assess specific vulnerabilities. Every vulnerability example includes a summary and a breakdown of the assessment. CVSS version 3.0 scores are provided to show differences between the two standards.

Details of the vulnerabilities and attacks were sourced primarily from the National Vulnerability Database (NVD) at https://nvd.nist.gov/vuln/search. Information from additional sources was also used when more details were required.

# Common Vulnerability Scoring System version 4.0 Examples

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of four metric groups: Base, Threat, Environmental, and Supplemental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Threat group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. Base metric values are combined with default values that assume the highest severity for Threat and Environmental metrics to produce a score ranging from 0 to 10. To further refine a resulting severity score, Threat and Environmental metrics can then be amended based on applicable threat intelligence and environmental considerations. Supplemental metrics do not modify the final score, and are used as additional insight into the characteristics of a vulnerability. A CVSS vector string consists of a compressed textual representation of the values used to derive the score. This document provides the official specification for CVSS version 4.0.

The most current CVSS resources can be found at https://www.first.org/cvss/

# New metric coverage

This section includes scoring examples that illustrate aspects of changed or modified metrics.

## New Metric – Attack Requirements

### CVE-2022-41741

A vulnerability in the module ngx_http_mp4_module might allow a local attacker to corrupt NGINX worker memory, resulting in its termination or potential other impact using a specially crafted audio or video file. The attack is only possible if an attacker can gain privileged access to the host running NGINX, place a specially crafted audio or video file within the webroot, and then trigger NGINX to process the specially crafted file.

| v3.1 | v4.0 Base |
|------|-----------|
| 7.0 | 7.3 |
| CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H | CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |

**CVSS v4 Score: Base 7.3**

| Metric | Value | Comments |
|--------|-------|----------|
| Attack Vector | Local | An attacker must be able to access the vulnerable system |

| | | with a local, interactive session. |
|---|---|---|
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | Present | Multiple conditions that require target specific reconnaissance and preparation must be satisfied in order to achieve successful exploitation of this vulnerability. |
| Privileges Required | Low | An attacker must be able to place a file within the web root to be processed by NGINX. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | The attacker could execute arbitrary code on the vulnerable system with elevated privileges. |
| Vulnerable System Integrity | High | The attacker could execute arbitrary code on the vulnerable system with elevated privileges. |
| Vulnerable System Availability | High | The attacker could execute arbitrary code on the vulnerable system with elevated privileges. |
| Subsequent System Confidentiality | None | There is no impact to the subsequent system confidentiality. |
| Subsequent System Integrity | None | There is no impact to the subsequent system integrity. |
| Subsequent System Availability | None | There is no impact to the subsequent system availability. |

## CVE-2020-3549

A vulnerability in the sftunnel functionality of Cisco Firepower Management Center (FMC) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to obtain the device registration hash.

The vulnerability is due to insufficient sftunnel negotiation protection during initial device registration. An attacker in a man-in-the-middle position could exploit this vulnerability by

intercepting a specific flow of the sftunnel communication between an FMC device and an FTD device. A successful exploit could allow the attacker to decrypt and modify the sftunnel communication between FMC and FTD devices, allowing the attacker to modify configuration data sent from an FMC device to an FTD device or alert data sent from an FTD device to an FMC device.

| | v3.1 | v4.0 |
|---|---|---|
| **Base** | 8.1<br>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H | 7.7<br>CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |
| **Base + Threat** | | 5.2<br>CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U |

## CVSS v4 Score: Base + Threat 5.2

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | Present | An attacker must be on-path to be able to intercept communications between affected systems. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | Passive | A user must be logged in and using the application for traffic to be generated that an attacker could capture. |
| Vulnerable System Confidentiality | High | An attacker could gain access to the system with a highly privileged user account. |
| Vulnerable System Integrity | High | An attacker could gain access to the system with a highly privileged user account. |

| | | |
|---|---|---|
| Vulnerable System Availability | High | An attacker could gain access to the system with a highly privileged user account. |
| Subsequent System Confidentiality | None | There is no impact to the vulnerable system confidentiality. |
| Subsequent System Integrity | None | There is no impact to the vulnerable system integrity. |
| Subsequent System Availability | None | There is no impact to the vulnerable system availability. |
| Exploit Maturity | Unreported | There is no known proof-of-concept code or malicious exploitation of this vulnerability. |

## CVE-2023-3089

Description: A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated.

| | v3.1 | v4.0 |
|---|---|---|
| **Base** | 7.5<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N | 8.3<br>CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N |
| **Base + Environmental** | | 8.1<br>CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N/CR:H/IR:L/AR:L/MAV:N/MAC:H/MVC:H/MVI:L/MVA:L |

**CVSS v4 Score: Base + Environmental 8.1**

| Metric | Value | Comments |
|---|---|---|

| | | |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | There is no inherent vulnerability, but a lower level of cryptography than expected was being used, resulting in a lower-than-configured certificate security. |
| Attack Requirements | Present | Attack requirements are present. Only applications built with a specific configuration are vulnerable. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | This CVE particularly affects high-security systems (FIPS users) and lowers the requirements to access confidential information. |
| Vulnerable System Integrity | Low | Integrity will be at a lower cryptographic level than desired, but is still always encrypted. |
| Vulnerable System Availability | Low | Integrity will be at a lower cryptographic level than desired, but is still always encrypted. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |
| Subsequent System Availability | None | There is no impact to subsequent systems. |
| Modified Attack Vector | Network | This still requires spoofing a cryptographically secure certificate, just not always an FIPS-approved algorithm. |
| Modified Attack Complexity | High | This still requires spoofing a cryptographically secure certificate, just not always an FIPS-approved algorithm. |
| Modified Vulnerable System Confidentiality | High | This still requires spoofing a cryptographically secure certificate, just not always an FIPS-approved algorithm. |
| Modified Vulnerable System Integrity | Low | Integrity will be at a lower cryptographic level than desired, but is still always encrypted. |
| Modified Vulnerable | Low | Integrity will be at a lower cryptographic level than desired, |

| System Availability | | but is still always encrypted. |
|---|---|---|
| Confidentiality Requirements | High | System certificates are still encrypted correctly, but at a weaker level than expected, resulting in a hard-to-abuse system, but easier than intended/designed for the system. |
| Integrity Requirements | Low | There is a low chance of integrity being modified, but higher than expected behavior. |
| Availability Requirements | Low | There is a low chance of availability being affected, but higher than expected behavior. |

# Revised Metric – User Interaction

Analysts assessing User Interaction should consider the necessary actions taken by a user. As per the specification document, operations normally taken by a user would be User Interaction:Passive. Actions that are out of the ordinary, against recommended guidance, or subverting security controls, would be User Interaction:Active.

## CVE-2021-44714

Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a Violation of Secure Design Principles that could lead to a Security feature bypass. Acrobat Reader DC displays a warning message when a user clicks on a PDF file, which could be used by an attacker to mislead the user. In affected versions, this warning message does not include custom protocols when used by the sender. User interaction is required to abuse this vulnerability as they would need to click 'allow' on the warning message of a malicious file.

| v3.1 | v4.0 Base |
|---|---|
| 3.3 | 4.6 |
| CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N | CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N |

**CVSS v4 Score: Base 4.6**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Local | The document must be present on the local disk. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | Active | User interaction is required to abuse this vulnerability because they would need to click **allow** on the warning message of a malicious file. |
| Vulnerable System Confidentiality | Low | Warning dialog messages do not contain all information about the document. Important omitted information about the document may allow the attacker to conduct further spoofing attacks. |
| Vulnerable System Integrity | None | There is no impact on vulnerable systems. |
| Vulnerable System Availability | None | There is no impact on vulnerable systems. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |
| Subsequent System Availability | None | There is no impact to subsequent systems. |

## CVE-2022-21830

Description A blind self XSS vulnerability exists in RocketChat LiveChat <v1.9 that could allow an attacker to trick a victim pasting malicious code in their chat instance.

| V3.1 | v4.0 Base |
|---|---|
|  |  |

| | |
|---|---|
| 6.1 | 5.1 |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N | [CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N](CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N) |

**CVSS v4 Score: Base 5.1**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | Active | The attacker must convince the user to input malicious script into the application. |
| Vulnerable System Confidentiality | None | No impact to the vulnerable application. |
| Vulnerable System Integrity | None | No impact to the vulnerable application. |
| Vulnerable System Availability | None | No impact to the vulnerable application. |
| Subsequent System Confidentiality | Low | An attacker could read data from the user's browser. |
| Subsequent System Integrity | Low | An attacker could modify data in the user's browser. |
| Subsequent System Availability | None | No direct availability impact to the user's browser. |

# New Metric – Subsequent Confidentiality, Availability, Integrity

Some examples of subsequent systems include:

- Guest host in a VMM hypervisor
- Device attached to a network gateway
- A managed Device
    - Including OT / ICS / SCADA equipment

## CVE-2022-22186

Due to an Improper Initialization vulnerability in Junos OS on EX4650 devices, packets received on the em0 but not destined to the device, may be improperly forwarded to an egress interface, instead of being discarded. Such traffic being sent by a client may appear genuine, but is non-standard in nature and should be considered as potentially malicious.

| v3.1 | v4.0 Base |
|---|---|
| 7.2 | 6.9 |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N |

**CVSS v4 Score: Base 6.9**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | An attacker must be able to access the vulnerable system with a local, interactive session. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | None | There is no impact to the vulnerable system confidentiality. |
| Vulnerable System Integrity | None | There is no impact to the vulnerable system integrity. |

| | | |
|---|---|---|
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |
| Subsequent System Confidentiality | Low | Network traffic or information from restricted hosts may be detected. |
| Subsequent System Integrity | Low | Network traffic may be sent to an undesired interface, impacting networks and other systems that should be restricted by the vulnerable system. |
| Subsequent System Availability | None | There is no impact to subsequent systems. |

## CVE-2023-21989

Description

Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attackers with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data.

| v3.1 | v4.0 Base |
|---|---|
| 6.0 | 5.9 |
| CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N | CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:N/SC:H/SI:N/SA:N |

## CVSS v4 Score: Base 5.9

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Local | An attacker must be able to access the vulnerable system with a local, interactive session. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |

| | | |
|---|---|---|
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | High | An attacker must have administrative control over a virtual machine within the virtual machine host. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | None | There is no impact to the vulnerable system confidentiality. |
| Vulnerable System Integrity | None | There is no impact to the vulnerable system integrity. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |
| Subsequent System Confidentiality | High | An attacker could exploit this vulnerability to access confidential information stored within the VM host hypervisor system. |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |
| Subsequent System Availability | None | There is no impact to subsequent systems. |

## CVE-2020-3947

VMware Workstation (15.x before 15.5.2) and Fusion (11.x before 11.5.2) contain a use-after vulnerability in vmnetdhcp. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition of the vmnetdhcp service running on the host machine.

| v3.1 | v4.0 Base |
|---|---|
| 9.3 | 9.4 |
| CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H | CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H |

**CVSS v4 Score: Base 9.4**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Local | An attacker must be able to access the vulnerable system with a local, interactive session. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | High | An attacker must have administrative control over a virtual machine within the virtual machine host. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | An attacker could execute arbitrary code on the vulnerable system, the hypervisor host. |
| Vulnerable System Integrity | High | An attacker could execute arbitrary code on the vulnerable system, the hypervisor host. |
| Vulnerable System Availability | High | An attacker could execute arbitrary code on the vulnerable system, the hypervisor host. |
| Subsequent System Confidentiality | High | An attacker could take actions on other virtualized guest systems hosted within the virtual hypervisor. |
| Subsequent System Integrity | High | An attacker could take actions on other virtualized guest systems hosted within the virtual hypervisor. |
| Subsequent System Availability | High | An attacker could take actions on other virtualized guest systems hosted within the virtual hypervisor. |
| Exploit Maturity | Proof-of-Concept (P) | A proof of concept is available |

## CVE-2023-48228

Description
authentik is an open-source identity provider. When initialising a oauth2 flow with a `code_challenge` and `code_method` (thus requesting PKCE), the single sign-on provider (authentik) must check if there is a matching and existing `code_verifier` during the token step. Prior to versions 2023.10.4 and 2023.8.5, authentik checks if the contents of `code_verifier` is

matching only when it is provided. When it is left out completely, authentik simply accepts the token request without it; even when the flow was started with a `code_challenge`. authentik 2023.8.5 and 2023.10.4 fix this issue.

| v3.1 | v4.0 Base |
|------|-----------|
| 7.5 | 9.3 |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:H/SI:H/SA:H |

## CVSS v4 Score: Base 9.4

| Metric | Value | Comments |
|--------|-------|----------|
| Attack Vector | Remote | An attacker must be able to send requests to a system using the vulnerable application. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | None | There is no impact to the vulnerable system confidentiality. |
| Vulnerable System Integrity | High | The attacker could cause the application to generate an arbitrary authentication token. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |
| Subsequent System Confidentiality | High | An attacker could potentially use a token generated by the vulnerable application to gain access to another system. |
| Subsequent System Integrity | High | An attacker could potentially use a token generated by the vulnerable application to gain access to another system. |

| | | |
|---|---|---|
| Subsequent System Availability | High | An attacker could potentially use a token generated by the vulnerable application to gain access to another system. |

## New Metric – Safety

Safety is a Supplemental metric which may be optionally assessed by a scoring provider with values of Not Defined (X), Present (P), or Negligible (N).  In the case of a system that intends to have health-related functions, it might also have a Safety-related consequence if a vulnerability is exploited.  Let's look at an example.

**CVE-2023-30560**

There are two known configurations of a product known as the Becton Dickinson PCU which can be modified without authentication using physical connection to the PCU.  A PCU is commonly used for infusion delivery in a healthcare provider environment.  With that context in mind, it could be inferred that an exploit of this vulnerability might have Safety impact.  The below is only an example of how this, or a similar vulnerability, *could* be scored.

| v3.1 | v4.0 Base |
|---|---|
| 6.8 | 8.3 |
| CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:H/SA:N/S:P/V:D |

**CVSS v4 Score: Base 8.3**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Physical | An attacker must be able to physically access the system. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | An attacker is unauthorized prior to the attack. |
| User Interaction | None | No user interaction is required for an attacker to |

| | | successfully exploit the vulnerability. |
|---|---|---|
| Vulnerable System Confidentiality | High | An attacker could execute arbitrary code on the vulnerable system. |
| Vulnerable System Integrity | High | An attacker could execute arbitrary code on the vulnerable system. |
| Vulnerable System Availability | High | An attacker could execute arbitrary code on the vulnerable system. |
| Subsequent System Confidentiality | None | If the scoring provider assumes that a patient is the subsequent system, a successful exploit would not result in loss of confidentiality. |
| Subsequent System Integrity | High | If the scoring provider assumes that a patient is the subsequent system, a successful exploit could result in loss of health integrity for that patient. |
| Subsequent System Availability | None | If the scoring provider assumes that a patient is the subsequent system, the attribute of availability might be metaphorically ambiguous. |

## CVSS v4 Supplemental Metrics

| Metric | Value | Comments |
|---|---|---|
| Safety | Present | Consequences of exploiting this vulnerability could have a Safety impact that is equal to or worse than "marginal", as described in IEC 61508. |
| Value Density | Diffuse | The system with the vulnerable component is fairly limited in resources. |

# CISA KEV Examples

This section will list a rotating sample of CVEs published as part of the CISA KEV list.

## CVE-2025-24201

Description

An out-of-bounds write issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in visionOS 2.3.2, iOS 18.3.2 and iPadOS 18.3.2, macOS Sequoia 15.3.2, Safari 18.3.1. Maliciously crafted web content may be able to break out of Web Content sandbox. This is a supplementary fix for an attack that was blocked in iOS 17.2. (Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 17.2.).

| v3.1 | v4.0 Base+Threat |
|---|---|
| 7.1 | 7.3 |
| CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H | CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A |

## CVSS v4 Score: Base+Threat 7.3

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Remote | An attacker must be able to send requests to a system using the vulnerable application. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | Present | Some unidentified attack requirements, such as timing requirements, may be present or attacks may be unreliable and not work every time. |
| Privileges Required | Low | Attackers require some measure of undetermined privileges to access the vulnerable application. |
| User Interaction | Active | Attackers must convince users to access malicious content using a browser application on an affected system. |
| Vulnerable System Confidentiality | High | Attackers could bypass sandbox protections and take privileged actions on the underlying operating system. |
| Vulnerable System Integrity | High | Attackers could bypass sandbox protections and take privileged actions on the underlying operating system. |

| Vulnerable System Availability | High | Attackers could bypass sandbox protections and take privileged actions on the underlying operating system. |
|---|---|---|
| Subsequent System Confidentiality | None | There is no impact to subsequent system confidentiality. |
| Subsequent System Integrity | None | There is no impact to subsequent system integrity. |
| Subsequent System Availability | None | There is no impact to subsequent system availability. |
| Threat | Attacked | The vendor indicates the vulnerability has been used in limited, targeted attacks. |

# Classic Examples

These were in the previous version and we are carrying them forward to show the change between version 3 and 4.

## OpenSSL Heartbleed Vulnerability (**CVE-2014-0160**)

### Vulnerability

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

### Attack

A successful attack requires only sending a specially crafted message to a web server running OpenSSL. The attacker constructs a malformed "heartbeat request" with a large field length and small payload size. The vulnerable server does not validate  the length of the payload against the provided field length and will return up to 64 kB of server memory to the attacker. It is likely that this memory was previously utilized by OpenSSL. Data returned may contain

sensitive information such as encryption keys or user names and passwords that could be used by the attacker to launch further attacks

| v3.1 Base | v3.1 Base + Temporal | v4.0 Base + Threat |
|---|---|---|
| 7.5 | 7.0 | 8.7 |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:A |

## CVSS v4 Score: Base + Threat 8.7

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | Access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact to the affected scope (e.g. the attacker can read the administrator's password, or private keys in memory are disclosed to the attacker). |
| Vulnerable System Integrity | None | There is no impact to the vulnerable system integrity. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System | None | There is no impact to subsequent systems. |

| Integrity | | |
|---|---|---|
| Subsequent System Availability | None | There is no impact to subsequent systems. |
| Exploit Maturity | Attacked | There are known exploits in the wild. |

# Apache log4j JNDI Command Execution "log4shell" Vulnerability (**CVE-2021-44228**)

A vulnerability in the Apache log4j library could allow an unauthenticated, remote attacker to execute arbitrary commands with the privileges of the service using the vulnerable library.

Notes:
In most circumstances all impacts to this vulnerability are constrained to the vulnerable system using the vulnerable library. This example has been updated to indicate impacts only to the vulnerable system.

| v3.1 Base | v4.0 Base + Threat |
|---|---|
| 10.0 | 9.3 |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A |

**CVSS v3.1 Base Score: 10.0**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerability is in a network service that uses log4j. |
| Attack Complexity | Low | No conditions outside of the user's control. |
| Privileges Required | None | An attacker requires no privileges to mount an attack. |
| User Interaction | None | The attacker requires no user interaction to successfully exploit the vulnerability |

| | | |
|---|---|---|
| Scope | Changed | The vulnerable component could allow an attacker to affect downstream components and systems. |
| Confidentiality | High | An attacker can execute arbitrary commands with elevated privileges. |
| Integrity | High | An attacker can execute arbitrary commands with elevated privileges. |
| Availability | High | An attacker can execute arbitrary commands with elevated privileges. |

## CVSS v4 Score: Base + Threat 9.3

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | Although the attacker must prepare the environment to achieve the worst possible outcome of an attack, (for example, code execution) through control of a reachable LDAP server, the system should be assumed vulnerable. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | The attack does not require any user interaction. |
| Vulnerable System Confidentiality | High | The attacker can run arbitrary commands with elevated privileges and access sensitive system information. |
| Vulnerable System Integrity | High | The attacker can run arbitrary commands with elevated privileges and modify the system configuration. |
| Vulnerable System Availability | High | The attacker can run arbitrary commands with elevated privileges and gain access sufficient to reset or turn off the device. |
| Subsequent System Confidentiality | None | Impacts constrained to the vulnerable system. |
| Subsequent System | None | Impacts constrained to the vulnerable system. |

| Integrity | | |
|---|---|---|
| Subsequent System Availability | None | Impacts constrained to the vulnerable system. |
| Exploit Maturity | Attacked | There are known exploits in the wild. |

## GNU Bourne-Again Shell (Bash) 'Shellshock' Vulnerability (**CVE-2014-6271**)

Vulnerability
GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "Shellshock."

Attack
A successful attack can be launched by an attacker directly against the vulnerable GNU Bash shell, or in certain cases, by an unauthenticated, remote attacker through services either written in GNU Bash or services spawning GNU Bash shells. In the case of an attack against the Apache HTTP Server running dynamic content CGI modules, an attacker can submit a request while providing specially crafted commands as environment variables. These commands will be interpreted by the handler program, the GNU Bash shell, with the privilege of the running HTTPD process. As such, environment variables passed by the attacker could allow installation of software, account enumeration, denial of service, etc. Attacks against other services that have a relationship with the GNU Bash shell are similarly possible.

| v3.1 Base | v4.0 Base + Threat |
|---|---|
| 9.8 | 9.3 |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A |

## CVSS v3.1 Base Score: 9.8

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The reasonable worst-case scenario is a network attack through a web server. |
| Attack Complexity | Low | An attacker needs only to gain access to a listening service that uses the GNU Bash shell as an interpreter or interact with a GNU Bash shell directly. |
| Privileges Required | None | The reasonable worst-case scenario is an attack through a web server, which does not require any privileges, for example, a simple CGI script. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Scope | Unchanged | The vulnerable component is the GNU Bash shell, which is used as an interpreter for various services or can be accessed directly. It runs within the security authority of the operating system. The impacted component is also the operating system, so there is no scope change. |
| Confidentiality | High | An attacker can take complete control of the affected system. |
| Integrity | High | An attacker can take complete control of the affected system. |
| Availability | High | An attacker can take complete control of the affected system. |

## CVSS v4 Score: Base + Threat 9.3

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully |

| | | exploit the vulnerability. |
|---|---|---|
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | The attacker can run arbitrary commands with elevated privileges and access sensitive system information. |
| Vulnerable System Integrity | High | The attacker can run arbitrary commands with elevated privileges and modify the system configuration. |
| Vulnerable System Availability | High | The attacker can run arbitrary commands with elevated privileges and gain access sufficient to reset or turn off the device. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |
| Subsequent System Availability | None | There is no impact to subsequent systems. |
| Exploit Maturity | Attacked | There are known exploits in the wild. |

# Juniper Proxy ARP Denial of Service Vulnerability (CVE-2013-6014)

**Vulnerability**

If Proxy ARP is enabled on an unnumbered interface, an attacker can poison the ARP cache and create a bogus forwarding table entry for an IP address, effectively creating a denial of service for that subscriber or interface. When Proxy ARP is enabled on an unnumbered interface, the router will answer any ARP message from any IP address which could lead to exploitable information disclosure. This issue can affect any product or platform running Junos OS 10.4, 11.4, 11.4X27, 12.1, 12.1X44, 12.1X45, 12.2, 12.3, or 13.1, supporting unnumbered interfaces.

**Attack**

Exploitation of this vulnerability requires network adjacency with the target system and the ability to generate arbitrary ARP replies sent to the connected interface. A rogue subscriber

can poison the ARP cache and/or create a rogue forwarding table entry for an IP of choice, effectively obscuring that IP address or redirecting IP traffic to the attacker.

The resultant impact can be observed as unauthorized modification of a database on the vulnerable component, or as an impact on confidentiality or availability on attached devices (impacted component). Since the CVSSv3 score for a high confidentiality (or availability) impact on a changed scope is higher than a partial impact on the vulnerable component, CVSSv3 guidance recommends to score for the higher overall impact.

| v3.1 | v4.0 Base |
|---|---|
| 9.3 | 6.4 |
| CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:H | CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:H/SI:N/SA:H |

## CVSS v4 Score: Base 6.4

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Adjacent | The attacker must be within the local proximity of the device. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | None | There is no impact to the vulnerable system confidentiality. |
| Vulnerable System Integrity | Low | Unauthorized modification of a database on the vulnerable system. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |
| Subsequent System | High | The attacker can hijack and redirect the IP traffic to |

| Confidentiality | | themselves. |
|---|---|---|
| Subsequent System Integrity | None | There is no impact to the subsequent system integrity. |
| Subsequent System Availability | High | Adding the rogue forwarding table can redirect the end user to rogue IP addresses. |

# Lenovo ThnkPwn Exploit (**CVE-2016-5729**)

Vulnerability

The SmmRuntime BIOS EFI Driver allows local administrators to execute arbitrary code with System Management Mode (SMM) privileges via unspecified vectors.

Attack

Attacker creates a buffer in memory containing exploit code to be executed in SMM context. Attacker then creates a structure with a pointer to the exploit code's entry point and triggers an SMI passing a reference to that structure. The SMM driver then calls the exploit code via the supplied function pointer.

Notes:

The previous assessment that notes impacts to subsequent systems was based on outdated understanding from CVSS 3.1. A new consensus has evolved with the understanding that hardware, firmware, and software running on a physical device in most cases are considered a single system, per definition in the CVSS Specification Document section 2.2 and the definition of a system of interest.

| v3.1 | v4.0 Base + Threat |
|---|---|
| 8.2 | 8.4 |
| CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H | CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/R:I |

**CVSS v4 Score: Base + Threat 9.3**

| Metric | Value | Comments |
|---|---|---|

| Attack Vector | Local | An attacker must be able to execute code on the system. |
|---|---|---|
| Attack Complexity | Low | This attack leverages a failure to verify input parameters in the **SmmRuntime** driver and can be reproduced consistently with simple code. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | High | The attacker must be able to run kernel level (ring 0) code on the affected system. |
| User Interaction | None | The vulnerability is built into the BIOS and is always available. There is no user configuration involved. |
| Vulnerable System Confidentiality | High | SMM has complete control over the system, including all information on the system. |
| Vulnerable System Integrity | High | SMM access allows an attacker to modify any part of the system. |
| Vulnerable System Availability | High | The attacker could keep the system in SMM, denying access to the system and never returning to a normal operation mode. |
| Subsequent System Confidentiality | None | While impacts may be expanded from BIOS to any operating system running on the device, the combination of hardware, firmware and software is considered a singular system as defined by a system of interest. |
| Subsequent System Integrity | None | Impacts constrained to the vulnerable system. |
| Subsequent System Availability | None | Impacts constrained to the vulnerable system. |
| Recovery | Irrecoverable | The attacker could keep the system in SMM, and could prevent recovery of the system by automatically running their code and locking down the system to prevent a user from accessing it. |

# Failure to Lock Flash on Resume from sleep (**CVE-2015-2890**)

Vulnerability

Some UEFI BIOS implementations failed to set Flash write protections such as the BIOS_CNTL locking on resume from the S3 suspend to RAM sleep state.

Attack
Attacker causes or waits until the system resumes from suspend, and then writes over the current BIOS image in Flash with a new BIOS image modified by the attacker.

| v3.1 | v4.0 Base + Threat |
|------|--------------------|
| 6.0 | 7.1 |
| CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H | CVSS:4.0/AV:L/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/R:I |

## CVSS v4 Score: Base + Threat 8.7

| Metric | Value | Comments |
|--------|-------|----------|
| Attack Vector | Local | An attacker must be able to execute code on the system. |
| Attack Complexity | Low | An attacker has unfettered access to the Flash part on which the BIOS is stored. |
| Attack Requirements | Present | The vulnerability is introduced by firmware failing to enable correct flash memory protections upon the resume from S3 system sleep state. |
| Privileges Required | High | An attacker must be able to run kernel level (ring 0) code on the target system, in order to access the Flash part. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | An attacker that can modify the BIOS image can install components to completely monitor and control the vulnerable system. |
| Vulnerable System Integrity | High | An attacker that can modify the BIOS image can modify anything on the vulnerable system. |
| Vulnerable System | High | An attacker could cause a denial of service by corrupting |

| | | |
|---|---|---|
| Availability | | the BIOS image or could encrypt the vulnerable system. |
| Subsequent System Confidentiality | None | Impacts constrained to the vulnerable system. |
| Subsequent System Integrity | None | Impacts constrained to the vulnerable system. |
| Subsequent System Availability | None | Impacts constrained to the vulnerable system. |
| Recovery | Irrecoverable | An attacker could cause a denial of service through encryption or corruption, neither of which could be fixed by a user. |

# Intel DCI Issue (**CVE-2018-3652**)

Vulnerability
Existing UEFI setting restrictions for DCI (Direct Connect Interface) in 5th and 6th generation Intel Xeon Processor E3 Family, Intel Xeon Scalable processors, and Intel Xeon Processor D Family allows a limited physical presence attacker to potentially access platform secrets via debug interfaces.

Attack
An attacker with physical access can attach a debug device to the DCI interface and directly interrogate and control the processor state starting from very early in the boot process.

| v3.1 | v4.0 Base |
|---|---|
| 7.6 | 7.0 |
| CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H | CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |

**CVSS v4 Score: Base 8.6**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Physical | An attacker must have physical access to the DCI port in order to attach the debugging device. |
| Attack Complexity | Low | The debugging device is off-the-shelf hardware that can be purchased from Intel. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | Only physical presence is required; no system privileges are required. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | An attacker can view all memory and CPU instructions. |
| Vulnerable System Integrity | High | An attacker can modify all contents of memory and control the CPU directly. |
| Vulnerable System Availability | High | An attacker can cause a denial of service by stopping the CPU from executing the desired functionality. |
| Subsequent System Confidentiality | None | Impacts constrained to the vulnerable system. |
| Subsequent System Integrity | None | Impacts constrained to the vulnerable system. |
| Subsequent System Availability | None | Impacts constrained to the vulnerable system. |

# Common Vulnerabilities Classes

This section contains examples of commonly-seen vulnerabilities from across the industry. The examples here are meant to be illustrative of common issues, but should not be considered authoritative. Unique vulnerabilities may have different impacts.

Note as well that some examples show the use of Threat and Environmental scores. Threat and Environmental metrics should typically only be used by CVSS consumers. The Threat and Environmental metrics shown here illustrate how to use the metrics.

# regreSSHion – **CVE-2024-6387**

Description

A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead to sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

Notes:

The scenario below assumes a standalone Linux-based system without dependent managed systems that has ASLR protections enabled.

| v3.1 | v4.0 Base+Threat |
|------|------------------|
| 8.1 | 8.2 |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H | CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P |

## CVSS v4 Score: Base 8.2

| Metric | Value | Comments |
|--------|-------|----------|
| Attack Vector | Network | An attacker must be able to connect to the system from a remote network. |
| Attack Complexity | High | Attackers must be able to defeat mitigations on platforms where ASLR and other memory defenses are present. |
| Attack Requirements | Present | An attacker must defeat a race condition, making the exploit unreliable. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to |

| | | successfully exploit the vulnerability. |
|---|---|---|
| Vulnerable System Confidentiality | High | The attacker could execute arbitrary code, which could allow the attacker to completely compromise the affected system. |
| Vulnerable System Integrity | High | The attacker could execute arbitrary code, which could allow the attacker to completely compromise the affected system. |
| Vulnerable System Availability | High | The attacker could execute arbitrary code, which could allow the attacker to completely compromise the affected system. |
| Subsequent System Confidentiality | None | There is no direct impact to subsequent systems. |
| Subsequent System Integrity | None | There is no direct impact to subsequent systems. |
| Subsequent System Availability | None | There is no direct impact to subsequent systems. |
| Exploit Maturity | Proof-of-concept | A proof-of-concept that demonstrates the vulnerability is available publicly. |

**Variation 1: Login Mitigation**

In this variation, the application of the mitigation to reduce LoginGraceTime to 0 prevents exploitation of arbitrary code execution. However, the modified configuration leaves the SSH service vulnerable to resource exhaustion attacks. The resulting assessment reflects only the potential to cause a denial of service (DoS) condition.

The below score uses modified base metrics to reflect the changes to exploitability and impact values.

Modified Attack Complexity and Modified Attack Requirements replace the base Attack Complexity and Attack Requirements. With the mitigation in place, an attacker must no longer defeat a race condition or memory protections to exhaust available connections.

Modified Vulnerable System Confidentiality and Modified System Integrity values replace the base Vulnerable System Confidentiality and Vulnerable System Integrity. There are no longer impacts to system confidentiality or integrity with the mitigation in place.

| v3.1 | v4.0 Base+Threat+Environmental |
|------|-------------------------------|
| 8.1 | 5.5 |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H | [CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/MAC:L/MAT:N/MVC:N/MVI:N/MVA:L](#) |

## CVSS v4 Score: BTE 5.5

| Metric | Value | Comments |
|--------|-------|----------|
| Attack Vector | Network | An attacker can connect to the system from a remote network. |
| Attack Complexity | High | Attackers must be able to defeat mitigations on platforms where ASLR and other memory defenses are present. |
| Attack Requirements | Present | An attacker must defeat a race condition, making the exploit unreliable. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | The attacker could execute arbitrary code, which could allow the attacker to completely compromise the affected system. |
| Vulnerable System Integrity | High | The attacker could execute arbitrary code, which could allow the attacker to completely compromise the affected system. |
| Vulnerable System Availability | High | The attacker could execute arbitrary code, which could allow the attacker to completely compromise the affected system. |
| Subsequent System Confidentiality | None | There is no direct impact to subsequent systems. |
| Subsequent System Integrity | None | There is no direct impact to subsequent systems. |

| | | |
|---|---|---|
| Subsequent System Availability | None | There is no direct impact to subsequent systems. |
| Exploit Maturity | Proof-of-concept | A proof-of-concept that demonstrates the vulnerability is available publicly. |
| Modified Vulnerable System Confidentiality | None | With the mitigation in place, the attacker cannot impact system confidentiality. |
| Modified Vulnerable System Integrity | None | With the mitigation in place, the attacker cannot impact system integrity. |
| Modified Vulnerable System Availability | Low | The attacker could exhaust available connections, rendering the SSH service unavailable. |

# SQL Injection – **CVE-2023-30545**

Description

PrestaShop is an Open Source e-commerce web application. Prior to versions 8.0.4 and 1.7.8.9, it is possible for a user with access to the SQL Manager (Advanced Options -> Database) to arbitrarily read any file on the operating system when using SQL function `LOAD_FILE` in a `SELECT` request. This gives the user access to critical information. A patch is available in PrestaShop 8.0.4 and PS 1.7.8.9

| v3.1 | v4.0 Base |
|---|---|
| 6.5 | 7.1 |
| CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N |

**CVSS v4 Score: Base 7.1**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are |

| | | required. |
|---|---|---|
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | Low | Attacker has to have database access (non-root user access). |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | An attacker can read any file on the operating system |
| Vulnerable System Integrity | None | There is no impact to the vulnerable system integrity. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems Confidentiality. |
| Subsequent System Integrity | None | There is no impact to subsequent systems Integrity. |
| Subsequent System Availability | None | There is no impact to subsequent systems Availability. |

## On-path Attacker – **CVE-2021-23846**

Description
Firmware for Bosch devices transmits in clear text over HTTP, allowing on-path attackers to gain access to user credentials.

| v3.1 | v4.0 Base |
|---|---|
| 5.9 | 8.2 |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N |

**CVSS v4 Score: Base 8.2**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | Present | An attacker must be on-path to be able to intercept communications between affected systems. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | An attacker could access plain text user credentials. |
| Vulnerable System Integrity | None | There is no impact to the vulnerable system integrity. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |
| Subsequent System Availability | None | There is no impact to subsequent systems. |

# Denial of Service – **CVE-2023-22394**

Description
Memory leak due to receipt of specially crafted SIP calls (CVE-2023-22394)
An Improper Handling of Unexpected Data Type vulnerability in the handling of SIP calls in Junos OS on SRX Series and MX Series platforms allows an attacker to cause a memory leak leading to Denial of Services (DoS).

| | v3.1 | v4.0 |
|---|---|---|
| **Base** | 7.5<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H | 8.7<br>CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L |
| **Base + Threat** | | 6.6<br>CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L/E:U |

## CVSS v4 Score: Base + Threat 6.6

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | None | There is no impact to the vulnerable system confidentiality. |
| Vulnerable System Integrity | None | There is no impact to the vulnerable system integrity. |
| Vulnerable System Availability | High | An **Improper Handling of Unexpected Data Type** vulnerability in the handling of SIP calls in Juniper Networks Junos OS on SRX Series and MX Series platforms allows an attacker to cause a memory leak leading to denial of service. |
| Subsequent System | None | There is no confidentiality impact to subsequent systems. |

| | | |
|---|---|---|
| Confidentiality | | |
| Subsequent System Integrity | None | There is no impact to the integrity of subsequent systems. |
| Subsequent System Availability | Low | The subsequent device could be unavailable/unreachable for a brief period of time. |
| Exploit Maturity | Unreported | There is no known proof-of-concept or malicious exploitation of this vulnerability. |

# Cross-Site Scripting (Reflected) – **CVE-2022-24682**

Categories: XSS

An issue was discovered in the Calendar feature in Zimbra Collaboration Suite 8.8.x before 8.8.15 patch 30 (update 1), as exploited in the wild starting in December 2021. An attacker could place HTML containing executable JavaScript inside element attributes. This markup becomes unescaped, causing arbitrary markup to be injected into the document.

| v3.1 | v4.0 Base |
|---|---|
| 6.1 | 5.1 |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L /I:L/A:N | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/ SI:L/SA:N |

## CVSS v4 Score: Base 5.1

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |

| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
|---|---|---|
| User Interaction | Active | A targeted user must click a malicious link that is provided by an attacker. |
| Vulnerable System Confidentiality | None | There is no direct impact to the web application confidentiality. |
| Vulnerable System Integrity | None | There is no direct impact to the web application integrity. |
| Vulnerable System Availability | None | There is no direct impact to the web application availability. |
| Subsequent System Confidentiality | Low | An attacker could read data from the user's browser. |
| Subsequent System Integrity | Low | An attacker could modify data in the user's browser. |
| Subsequent System Availability | None | There is no direct availability impact to the user's browser. |

**Variation 1: Impact to Vulnerable Application**

Typical cross-site scripting CVSS assessments show simple, direct impacts to a user's browser. Some evaluations, however, may expand impacts to the vulnerable web application to show how an attacker can use access in the user's browser to impact the vulnerable web application. An example of this evaluation, a variant of CVE-2022-24682 based on reported attacks in the wild, is shown below.

| v4.0 Base |
|---|
| 5.1 |
| CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N |

**CVSS v4 Score: Base+Threat 5.1**

| Metric | Value | Comments |
|---|---|---|

| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
|---|---|---|
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | Active | A targeted user must click a malicious link that is provided by an attacker. |
| Vulnerable System Confidentiality | Low | User sessions could be abused to extract data from the application, including email content. |
| Vulnerable System Integrity | Low | User privileges could be abused to modify or delete data from the application, or send emails as a targeted user. |
| Vulnerable System Availability | None | No direct identified vulnerable system availability impact. |
| Subsequent System Confidentiality | Low | An attacker could read data from the user's browser. |
| Subsequent System Integrity | Low | An attacker could modify data in the user's browser. |
| Subsequent System Availability | None | There is no direct availability impact to the user's browser. |
| Threat | Reported | Reported by the vendor to be used in attacks. |

## Cross-Site Scripting (Stored) – **CVE-2020-0926**

Microsoft Office SharePoint XSS Vulnerability

Description
A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'.

An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.

| v3.1 | v4.0 Base |
|---|---|
| 5.4 | 5.1 |
| CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N |

## CVSS v4 Score: Base 5.1

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | Low | The attacker requires privileges sufficient to store data within the application. |
| User Interaction | Passive | A targeted user must browse to the application as part of normal operations. |
| Vulnerable System Confidentiality | None | There is no direct impact to the web application confidentiality. |
| Vulnerable System Integrity | None | There is no direct impact to the web application integrity. |
| Vulnerable System Availability | None | There is no direct impact to the web application availability. |

| | | |
|---|---|---|
| Subsequent System Confidentiality | Low | An attacker can read content that the attacker is not authorized to read from the user's browser. |
| Subsequent System Integrity | Low | An attacker could inject malicious content that could be executed within the user's browser. |
| Subsequent System Availability | None | There is no direct impact to the user's browser availability. |

## Cross-Site Scripting Expanded Impact – **CVE-2024-55228**

Categories: XSS
A cross-site scripting (XSS) vulnerability in the Product module of Dolibarr v21.0.0-beta allows attackers to execute arbitrary web scripts or HTMl via a crafted payload injected into the Title parameter.

Like other cross-site scripting examples as evaluated in CVSS vectors, the vulnerable system is defined as the web application that allows attackers to pass unfiltered input to the subsequent system, a browser application on a targeted user's system. This scoring example demonstrates an expanded impact from the targeted user's browser to the vulnerable application.

Note that this example may be atypical of cross-site scripting vulnerabilities. Depending on the privileges of the user who participates in an attack, impacts on the vulnerable application may differ or be entirely nonexistent. Assessments that include impacts to the vulnerable application should make certain to clearly define and document application impacts as a result of cross-site scripting exploitation.

| v3.1 | v4.0 Base |
|---|---|
| 9.0 | 8.5 |
| CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H /I:H/A:H | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:L/ SI:L/SA:N |

## CVSS v4 Score: Base 8.5

| Metric | Value | Comments |
|---|---|---|

| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
|---|---|---|
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | Low | An attacker requires privileges sufficient to access the vulnerable application. |
| User Interaction | Active | A targeted user must interact with an embedded element in the application that is provided by an attacker. |
| Vulnerable System Confidentiality | High | The attacker could trigger the execution of commands with the privileges of the targeted user, which could allow the attacker to gain access to sensitive information. |
| Vulnerable System Integrity | High | The attacker could trigger the execution of commands with the privileges of the targeted user, which could allow the attacker to modify the configuration or remove files. |
| Vulnerable System Availability | High | The attacker could trigger the execution of commands with the privileges of the targeted user, which could allow the attacker to disable features and impact system availability. |
| Subsequent System Confidentiality | Low | An attacker could read data from the user's browser. |
| Subsequent System Integrity | Low | An attacker could modify data in the user's browser. |
| Subsequent System Availability | None | There is no direct availability impact to the user's browser. |

## Cross-Site Request Forgery – **CVE-2023-5602**

WordPress Social Media Share Buttons & Social Sharing Icons Cross-Site Request Forgery

Description
The Social Media Share Buttons & Social Sharing Icons plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.8.5. This is due to missing or incorrect nonce validation on several functions corresponding to AJAX actions. This makes it

possible for unauthenticated attackers to invoke those actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

| v3.1 | v4.0 Base |
|---|---|
| 4.3 | 5.1 |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N |

## CVSS v4 Score: Base 5.1

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | Active | A targeted user must actively click on a malicious link that is provided by an attacker to initiate the attack sequence. |
| Vulnerable System Confidentiality | None | There is no direct impact to the web application confidentiality. |
| Vulnerable System Integrity | Low | The attacker could modify some values within the web application. |
| Vulnerable System Availability | None | There is no direct impact to the web application availability. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |
| Subsequent System | None | There is no impact to subsequent systems. |

| Availability | | |
|---|---|---|

# Privilege Escalation (Unprivileged) **CVE-2022-20759**

Description

Cisco Adaptive Security Appliance Firepower Threat Defense (FTD) Privilege Escalation Vulnerability (CVE-2022-20759)

A vulnerability in the web services interface for remote access VPN features of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, but unprivileged, remote attacker to elevate privileges to level 15.

An attacker could exploit this vulnerability by sending crafted HTTPS messages to the web services interface of an affected device. A successful exploit could allow the attacker to gain privilege level 15 access to the web management interface of the device.

| v3.1 | v4.0 Base |
|---|---|
| 8.8 | 7.7 |
| CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |

## CVSS v4 Score: Base 7.7

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | Attacks are executed through HTTPS requests. |
| Attack Complexity | Low | No advanced knowledge is required |
| Attack Requirements | Present | HTTP Management Access *and* IKEv2 Client Service must be enabled on at least one interface, or HTTP management interface *and* WebVPN must be enabled on at least one interface. |
| Privileges Required | Low | An attacker must have valid credentials for the VPN. |
| User Interaction | None | No additional user interaction is required for successful exploitation. |

| Vulnerable System Confidentiality | High | Successful exploitation could result in a complete compromise (enable 15) of the targeted device, which results in a complete (High) impact on the confidentiality of the device. |
|---|---|---|
| Vulnerable System Integrity | High | Successful exploitation could result in a complete compromise resulting in High integrity impact. |
| Vulnerable System Availability | High | Successful exploitation could result in a complete compromise resulting in High availability impact. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |
| Subsequent System Availability | None | There is no impact to subsequent systems. |

## Privilege Escalation (Highly Privileged) **CVE-2021-34724**

Description

A vulnerability in the Cisco IOS XE SD-WAN Software CLI could allow an authenticated, local attacker to elevate privileges and execute arbitrary code on the underlying operating system as the root user. An attacker must be authenticated on an affected device as a PRIV15 administrative user.

|  | **v3.1** | **v4.0** |
|---|---|---|
| **Base** | 6.0 CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N | 8.3 CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N |
| **Base + Threat** |  | 5.6 |

| | | CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U |
|---|---|---|

## CVSS v4 Score: Base + Threat 5.6

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Local | An attacker must be able to access the vulnerable system with a local, interactive session. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | High | An attacker must have administrator privileges within the affected system. |
| User Interaction | None | No additional user interaction is required for exploit |
| Vulnerable System Confidentiality | High | An attacker could execute arbitrary commands on the affected system with the privileges of the *root* user, allowing the privileged attacker to access sensitive files that would otherwise be inaccessible to the administrative user. |
| Vulnerable System Integrity | High | An attacker could execute arbitrary commands on the affected system with the privileges of the *root* user, allowing the privileged attacker to modify system values that would otherwise be inaccessible to the administrative user. |
| Vulnerable System Availability | None | An attacker does not gain any additional privileges to impact system availability. Privileges required to exploit this vulnerability already allow the attacker to turn off the system, so there is no privilege gain as a result of exploitation. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |

| | | |
|---|---|---|
| Subsequent System Availability | None | There is no impact to subsequent systems. |
| Exploit Maturity | Unreported | There is no known proof-of-concept code or malicious exploitation of this vulnerability. |

# Remote Code Execution (**CVE-2023-28311**)

Microsoft Word Remote Code Execution Vulnerability

An attacker must send the user a malicious file and convince the user to open said file which results in RCE.

| v3.1 | v4.0 Base |
|---|---|
| 7.8 | 8.5 |
| CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |

## CVSS v4 Score: Base 8.5

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Local | The document must be present on the local disk. |
| Attack Complexity | Low | Nothing outside of the attacker's control. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | Passive | A user must open a document. |
| Vulnerable System Confidentiality | High | The attacker could execute arbitrary code, which could allow the attacker to compromise the affected system completely. |

| Vulnerable System Integrity | High | The attacker could execute arbitrary code, which could allow the attacker to compromise the affected system completely. |
|---|---|---|
| Vulnerable System Availability | High | The attacker could execute arbitrary code, which could allow the attacker to compromise the affected system completely. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |
| Subsequent System Availability | None | There is no impact to subsequent systems. |

## Arbitrary Code Execution **CVE-2022-22965**

Spring4shell

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

Attack

An RCE can be established by simply sending a series of malicious web requests to a web server running on a vulnerable version of Spring. Spring4Shell allows attackers to get arbitrary code execution in the context of the user that is running the vulnerable application. Once the attackers achieve RCE, they can install malware or can use the server as an initial foothold to escalate privileges and compromise the whole system, or even access subsequent backend systems that the vulnerable server has privileged access to.

| v3.1 | v4.0 Base + Threat |
|---|---|
| 9.8 | 9.2 |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A |

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | Present | A successful attack depends on the deployment and execution conditions of the vulnerable system. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | The vulnerability allows an attacker to execute arbitrary code in the context of the user that is running the vulnerable application and gain complete control over the system. |
| Vulnerable System Integrity | High | The vulnerability allows an attacker to execute arbitrary code in the context of the user that is running the vulnerable application and gain complete control over the system. |
| Vulnerable System Availability | High | The vulnerability allows an attacker to execute arbitrary code in the context of the user that is running the vulnerable application and gain complete control over the system. |
| Subsequent System Confidentiality | None | There is no immediate loss of confidentiality within the subsequent systems. But, based on how Spring is deployed in the target environment, the compromised server could be used as a pivot to leverage further. If there are subsequent impacts, they should be defined in environmental metrics. |
| Subsequent System Integrity | None | There is no immediate loss of integrity within the subsequent systems. But, based on how Spring is deployed in the target environment, the compromised server could be used as a pivot to leverage further. If there are subsequent impacts, they should be defined in |

| | | |
|---|---|---|
| | | environmental metrics. |
| Subsequent System Availability | None | There is no immediate loss of availability within the subsequent system. But, based on how Spring is deployed in the target environment, the compromised server could be used as a pivot to leverage further. If there are subsequent impacts, they should be defined in environmental metrics. |
| Exploit Maturity | Attacked | There are known exploits in the wild. |

# Physical Access (CVE-2022-20826)

A vulnerability in the secure boot implementation of Cisco Secure Firewalls 3100 Series that are running Cisco Adaptive Security Appliance (ASA) Software or Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated attacker with physical access to the device to bypass the secure boot functionality. This vulnerability is due to a logic error in the boot process. An attacker could exploit this vulnerability by injecting malicious code into a specific memory location during the boot process of an affected device. A successful exploit could allow the attacker to execute persistent code at boot time and break the chain of trust.

| v3.1 | v4.0 Base |
|---|---|
| 6.4 | 5.4 |
| CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H | CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |

## CVSS v4 Score: Base 5.4

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Physical | An attacker requires physical access to a vulnerable system. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |

| | | |
|---|---|---|
| Attack Requirements | Present | There are timing requirements outside the attacker's control, making exploit attempts unreliable. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | An attacker could inject malicious, unsigned code and execute arbitrary commands. |
| Vulnerable System Integrity | High | An attacker could inject malicious, unsigned code and execute arbitrary commands. |
| Vulnerable System Availability | High | An attacker could inject malicious, unsigned code and execute arbitrary commands. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |
| Subsequent System Availability | None | There is no impact to subsequent systems. |

## Information Disclosure – **CVE-2022-21500**

Description

Vulnerability in Oracle E-Business Suite (component: Manage Proxies). The supported version that is affected is 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle E-Business Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle E-Business Suite accessible data.

Note: Authentication is required for successful attack, however the user may be self-registered. Oracle E-Business Suite 12.1 is not impacted by this vulnerability. Customers should refer to the Patch Availability Document for details.

| **v3.1** | **v4.0 Base** |
|---|---|
| 7.5 | 8.7 |

| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N |
|---|---|

**CVSS v4 Score: Base 8.7**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | An attacker could exploit the vulnerability to access critical data that is stored within the vulnerable application. |
| Vulnerable System Integrity | None | There is no impact to the vulnerable system integrity. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |
| Subsequent System Availability | None | There is no impact to subsequent systems. |

# Information Disclosure - **CVE-2021-32570**

In Ericsson Network Manager (ENM) releases before 21.2, users belonging to the same AMOS authorization group can retrieve the data from certain log files. All AMOS users are considered to be highly privileged users in the ENM system and all must be previously defined and authorized by the Security Administrator. Those users can access some log's files, under a common path, and read information stored in the log's files in order to conduct privilege escalation.

| v3.1 | v4.0 Base |
|---|---|
| 4.9 | 6.9 |
| CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N | CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N |

## CVSS v4 Score: Base 6.9

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | High | An attacker must have membership in the AMOS authorization group sufficient to read data from log files. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | An attacker could exploit the vulnerability to view sensitive data within the application log files. |
| Vulnerable System Integrity | None | There is no impact to the vulnerable system integrity. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |
| Subsequent System | None | There is no impact to subsequent systems. |

| | | |
|---|---|---|
| Confidentiality | | |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |
| Subsequent System Availability | None | There is no impact to subsequent systems. |

## Command Injection (**CVE-2022-26134**)

Description

Atlassian Confluence Server and Data Center OGNL Injection Vulnerability (CVE-2022-26134)

In Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance.

A remote attacker could exploit it by requests injecting specially crafted OGNL templates in order to execute arbitrary code.

| **v3.1** | **v4.0 Base** |
|---|---|
| 9.8 | 9.3 |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |

### CVSS v4 Score: Base 9.3

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | Attacks are executed through HTTP(s) requests and are accessible from remote networks. |
| Attack Complexity | Low | No advanced knowledge is required |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |

| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
|---|---|---|
| Vulnerable System Confidentiality | High | Successful exploitation could result in a complete compromise (command execution as *root*) of the affected device, which results in a complete (High) impact on the confidentiality of the device. |
| Vulnerable System Integrity | High | Successful exploitation could result in a complete compromise (command execution as *root*) of the affected device, which results in a complete (High) impact on the integrity of the device. |
| Vulnerable System Availability | High | Successful exploitation could result in a complete compromise (command execution as *root*) of the affected device, which results in a complete (High) impact on the availability of the device. |
| Subsequent System Confidentiality | None | There are no additional impacts to subsequent systems. |
| Subsequent System Integrity | None | There are no additional impacts to subsequent systems. |
| Subsequent System Availability | None | There are no additional impacts to subsequent systems. |

## ACL Bypass (**CVE-2023-20245**)

A vulnerability in the per-user-override feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass a configured access control list (ACL) and allow traffic that should be denied to flow through an affected device. The vulnerability is due to a logic error that could occur when the affected software constructs and applies per-user-override rules. An attacker could exploit the vulnerability by connecting to a network through an affected device that has a vulnerable configuration. A successful exploit could allow the attacker to bypass the interface ACL and access resources that should be protected.

| v3.1 | v4.0 Base | v4.0 BTE |
|---|---|---|
| 5.8 | 6.9 | 2.7 |

| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E:U/CR:L/IR:L/AR:L |
|---|---|---|

**CVSS v4 Score: Base 6.9**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | None | There is no impact to the vulnerable system confidentiality. |
| Vulnerable System Integrity | None | There is no impact to the vulnerable system integrity. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System Integrity | Low | The attacker could send network traffic to downstream destinations that should otherwise be inaccessible. |
| Subsequent System Availability | None | There is no impact to subsequent systems. |

## Variation 1: ACL Bypass with Downstream Impacts

In this example, we imagine a scenario in which the failure of an ACL to protect internal systems could result in impact to downstream systems.

| v4.0 Base |
| --- |
| 7.8 |
| CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:L/SI:N/SA:H |

## CVSS v4 Score: Base 7.8

| Metric | Value | Comments |
| --- | --- | --- |
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | None | There is no impact to the vulnerable system confidentiality. |
| Vulnerable System Integrity | Low | The attacker could send network traffic through the device to downstream destinations that should otherwise be inaccessible. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |
| Subsequent System Confidentiality | Low | The attacker could gather information about or access services on subsequent systems. |
| Subsequent System | None | There is no impact to subsequent systems. |

| | | |
|---|---|---|
| Integrity | | |
| Subsequent System Availability | High | The attacker could send streams of network traffic that could overwhelm the subsequent system, resulting in a denial of service condition. |

**Variation 2: ACL Bypass in open or low-value network segment**

**CVSS v4 Score: BTE 2.7**

The following threat and environmental metrics further enrich the ACL Bypass (CVE-2023-20245) example. The scoring scenario demonstrates impacts to an affected device that provides filtering for an open network with systems of minimal value such as a testing environment or lab environment regularly re-imaged and that does not contain any sensitive data. The security requirements for systems within this network are Low, because they are not critical to the environment, and impacts would, per the CVSS Specification Document – "likely to have only a limited adverse effect on the organization or individuals associated with the organization." Refer to the Threat and Environmental metric choices that further enrich the CVSS vector in the table above.

| Metric | Value | Comments |
|---|---|---|
| Threat | Unreported | No known public exploit exists. |
| Confidentiality Requirements | Low | Networks impacted by this ACL bypass contain only low-value systems with non-sensitive data. |
| Integrity Requirements | Low | Networks impacted by this ACL bypass contain only low-value systems with non-sensitive data. |
| Availability Requirements | Low | Networks impacted by this ACL bypass contain only low-value systems with non-sensitive data. |

# Server-Side Request Forgery (SSRF) (**CVE-2024-1233**)

Description:

A flaw was found in  JwtValidator.resolvePublicKey in JBoss EAP, where the validator checks jku and sends a HTTP request. During this process, no whitelisting or other filtering behavior is performed on the destination URL address, which may result in a server-side request forgery (SSRF) vulnerability.

Notes:

Impacts for server-side request forgery vulnerabilities may depend on both the configuration of the vulnerable system as well as the presence of other systems in the environment that could be accessed as part of exploitation.

The vulnerable system is the JBoss application server, while subsequent systems may be other applications on the same host or different back-end systems that are reachable by the vulnerable application server.

| v3.1 | v4.0 |
|------|------|
| 7.3 | 6.9 |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:L/SI:L/SA:L |

## CVSS v4 Score: Base 6.9

| Metric | Value | Comments |
|--------|-------|----------|
| Attack Vector | Network | An attacker must be able to send requests to an application that implements the vulnerable JBoss EAP feature. |
| Attack Complexity | Low | No built-in security-enhancing conditions exist within the product to inhibit successful exploitation. |
| Attack Requirements | None | The attacker can execute the exploit with no specific difficulty. No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | None | There is no impact to the vulnerable system confidentiality. |
| Vulnerable System Integrity | Low | The attacker could cause the vulnerable system to send arbitrary HTTP requests. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |

| Subsequent System Confidentiality | Low | The attacker could cause the vulnerable system to send HTTP requests on the attacker's behalf to another system, potentially allowing the attacker to gain information about or from a subsequent system. |
|---|---|---|
| Subsequent System Integrity | Low | The attacker could send HTTP requests to another system and modify the application state of a subsequent system. |
| Subsequent System Availability | Low | The attacker could send HTTP requests to another system and potentially impact the availability of a subsequent system. |

**Variation 1:**

In this variation, the system implementing the vulnerable JBoss EAP application allows access only to limited endpoints, reducing the subsequent system impact to Confidentiality only, allowing the attacker to gather information about systems that should be unreachable. This represents a more typical impact of a SSRF vulnerability.

In the metric strings below, the Modified Subsequent System Integrity and Availability are selected as None and replace the base Subsequent System Integrity and Availability impacts.

| v3.1 | v4.0 |
|---|---|
| 7.3 | 6.9 |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:L/SI:L/SA:L/MSI:N/MSA:N |

**CVSS v4 Score: Base+Environmental 6.9**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | An attacker must be able to send requests to an application that implements the vulnerable JBoss EAP feature. |
| Attack Complexity | Low | No built-in security-enhancing conditions exist within the product to inhibit successful exploitation. |

| | | |
|---|---|---|
| Attack Requirements | None | The attacker can execute the exploit with no specific difficulty. No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | None | A user, other than the attacker, must be present for the vulnerability to be exploited. However, the actions taken by the user are typical, because a user must open a file within the vulnerable application. |
| Vulnerable System Confidentiality | None | There is no impact to the vulnerable system confidentiality. |
| Vulnerable System Integrity | Low | Exploitation of the vulnerability results in complete control of the vulnerable system. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |
| Subsequent System Confidentiality | Low | The attacker could cause the vulnerable system to send HTTP requests on the attacker's behalf to another system, potentially allowing the attacker to gain information about or from a subsequent system. |
| Subsequent System Integrity | Low | The attacker could send HTTP requests to another system and modify the application state of a subsequent system.<br><br>Note: the Modified Subsequent System Integrity replaces this metric. |
| Subsequent System Availability | Low | The attacker could send HTTP requests to another system and potentially impact the availability of a subsequent system.<br><br>Note: the Modified Subsequent System Availability replaces this metric. |
| Modified Subsequent System Integrity | None | No applications reachable by the vulnerable system accept HTTP requests, resulting in no integrity impact. |
| Modified Subsequent System Availability | None | No applications reachable by the vulnerable system accept HTTP requests, resulting in no availability impact. |

# Industrial Control Systems (ICS) (**CVE-2023-28728**)

Description:

In Panasonic Control FPWIN versions 7.6.0.3 and prior, a stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack (i.e., is a local variable or a parameter to a function) when a file is opened within the application.

| v3.1 | v4.0 |
|---|---|
| 7.8 | 8.5 |
| CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:P |

**CVSS v4 Score: Base 8.5**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Local | An attacker must be locally connected to the vulnerable system. |
| Attack Complexity | Low | No built-in security-enhancing conditions exist within the product to inhibit successful exploitation. |
| Attack Requirements | None | The attacker can execute the exploit with no specific difficulty. No attack requirements are present. |
| Privileges Required | None | No privileges are required for an attacker to successfully exploit the vulnerability. |
| User Interaction | Passive | A user, other than the attacker, must be present for the vulnerability to be exploited. However, the actions taken by the user are typical, because a user must open a file within the vulnerable application. |
| Vulnerable System Confidentiality | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |
| Vulnerable System Integrity | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |
| Vulnerable System Availability | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |

| Subsequent System Confidentiality | None | The impact on confidentiality is limited to the vulnerable system. No direct downstream impact is indicated. |
| Subsequent System Integrity | None | The impact on integrity is limited to the vulnerable system. No direct downstream impact is indicated. |
| Subsequent System Availability | None | The impact on availability is limited to the vulnerable system. No direct downstream impact is indicated. |
| Safety | Present | The impact from an attacker gaining full control of software that is running on a programmable logic controller (PLC) may meet the definition of IEC 61508 consequence category **marginal**, **critical** or **catastrophic** for certain usage of the PLC in an Operational Technology (OT) environment where humans may be harmed. |

## Operational Technology (OT) (**CVE-2022-47379**)

An authenticated, remote attacker may use an out-of-bounds write vulnerability in multiple CODESYS products in multiple versions to write data into memory which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

| v3.1 | v4.0 |
|---|---|
| 8.8 | 9.4 |
| CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/S:P/AU:Y/V:C/RE:L |

**CVSS v4 Score: Base 9.4**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Remote | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | The attacker can execute the exploit with no specific difficulty. No attack requirements are present. |
| Privileges Required | Low | The attacker must require privileges sufficient to access the |

| | | device. |
|---|---|---|
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |
| Vulnerable System Integrity | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |
| Vulnerable System Availability | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |
| Subsequent System Confidentiality | High | The attacker could impact the confidentiality of connected OT devices. |
| Subsequent System Integrity | High | The attacker could impact the integrity of connected OT devices. |
| Subsequent System Availability | High | The attacker could impact the availability of connected OT devices. |
| Safety | Present | Connections to OT devices can impact the safety of humans and may meet the definition of IEC 61508 consequence category **marginal**, **critical** or **catastrophic** for certain usage in an Operational Technology (OT) environment where humans may be harmed. |
| Automatable | Yes | Attacks against the vulnerability can be performed in an automated fashion with little oversight against multiple targets. |
| Value Density | Concentrated | The value of OT devices in a facility has a highly concentrated value as a target. |
| Vulnerability Response Effort | Low | A simple device reboot would correct the issue. |

**Variation 1: Elevator Operational Technology**

In this variation of the vulnerability, the vulnerable device manages an elevator. The following metric score variation demonstrates the possible impacts of an exploit against such a deployment.

| B+E v4.0 |
|---|
| 7.0 |
| CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:P/CR:L/IR:H/AR:L/MAV:L/MAC:H/MAT:N/MPR:N/MUI:N/MVC:N/MVI:H/MVA:L/MSC:N/MSI:S/MSA:L |

## Variation 1: CVSS v4 Score: B+E 7.0

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | The attacker can execute the exploit with no specific difficulty. No attack requirements are present. |
| Privileges Required | Low | The attacker must require privileges sufficient to access the device. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |
| Vulnerable System Integrity | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |
| Vulnerable System Availability | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |
| Subsequent System Confidentiality | High | The attacker could impact the confidentiality of connected OT devices. |
| Subsequent System Integrity | High | The attacker could impact the confidentiality of connected OT devices. |

| Subsequent System Availability | High | The attacker could impact the confidentiality of connected OT devices. |
|---|---|---|
| Modified Attack Vector | Local | The system is disconnected from the Internet. |
| Modified Attack Complexity | High | There are FW and Data Diodes that prevent access to the PLC. |
| Modified Attack Requirements | None | Same as Base. |
| Modified Privileges Required | Low | Same as Base. |
| Modified User Interaction | None | Same as Base. |
| Modified Vulnerable System Confidentiality | None | No sensitive information contained within the PLC. |
| Modified Vulnerable System Integrity | High | The attacker could modify the operation of the elevator. |
| Modified Vulnerable System Availability | Low | Loss of an elevator compensated by other facility features. |
| Modified Subsequent System Confidentiality | None | No sensitive information contained within the elevator device. |
| Modified Subsequent System Integrity | High | The attacker could modify the operation of the elevator. |
| Modified Subsequent System Availability | Low | Loss of an elevator compensated by other facility features. |
| Confidentiality Requirements | Low | The system contains no secrets and the requirement is reduced. |
| Integrity Requirements | High | There could be a high risk of injury during malfunction to operations. |
| Availability Requirements | Low | Facility redundancy of other elevators reduces the availability requirements. |

**Variation 2: Oil Field Facility Operational Technology**

In this variation of the vulnerability, the vulnerable device manages a facility such as an oil field. The following metric score variation demonstrates the possible impacts of an exploit against such a deployment.

| B+E v4.0 |
|---|
| 7.4 |
| [CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/MAV:A/MAC:H/MAT:N/MPR:L/MUI:N/MVC:L/MVI:H/MVA:H/MSC:L/MSI:S/MSA:S/CR:L/IR:H/AR:H/E:P](CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/MAV:A/MAC:H/MAT:N/MPR:L/MUI:N/MVC:L/MVI:H/MVA:H/MSC:L/MSI:S/MSA:S/CR:L/IR:H/AR:H/E:P) |

**Variation 1: CVSS v4 Score: B+E 7.4**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | The attacker can execute the exploit with no specific difficulty. No attack requirements are present. |
| Privileges Required | None | The attacker must require privileges sufficient to access the device. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |
| Vulnerable System Integrity | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |

| Vulnerable System Availability | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |
|---|---|---|
| Subsequent System Confidentiality | High | The attacker could impact the confidentiality of connected OT devices. |
| Subsequent System Integrity | High | The attacker could impact the confidentiality of connected OT devices. |
| Subsequent System Availability | High | The attacker could impact the confidentiality of connected OT devices. |
| Modified Attack Vector | Adjacent | The system is disconnected from the Internet. However there is a possibility for lateral control from nearby management systems. |
| Modified Attack Complexity | High | There are FW and Data Diodes that prevent access to the PLC. |
| Modified Attack Requirements | None | Same as Base. |
| Modified Privileges Required | Low | Same as Base. |
| Modified User Interaction | None | Same as Base. |
| Modified Vulnerable System Confidentiality | Low | The attacker could recover some information regarding facility data. |
| Modified Vulnerable System Integrity | High | The attacker could modify the operation of the facility. |
| Modified Vulnerable System Availability | High | The attacker could impact the availability of the PLC. |
| Modified Subsequent System Confidentiality | Low | The attacker could recover information regarding production facility data. |
| Modified Subsequent System Integrity | Safety | The attacker could modify the facility operations, possibly impacting the safety of facility personnel. |
| Modified Subsequent System Availability | Safety | The attacker could impact facility availability, possibly impacting the safety of facility personnel. |

| | | |
|---|---|---|
| Confidentiality Requirements | High | The device and facility may hold trade secrets. |
| Integrity Requirements | High | Improper operation of the facility could impact the safety of nearby personnel. |
| Availability Requirements | High | Equipment failure could result in facility downtime. |

**Variation 3: Assembly Line Robots Operational Technology**

In this variation of the vulnerability, the vulnerable device manages robotic devices in an assembly line. The following metric score variation demonstrates the possible impacts of an exploit against such a deployment.

| B+E v4.0 |
|---|
| 8.7 |
| CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/MAV:N/MAC:H/MAT:N/MPR:L/MUI:N/MVC:H/MVI:H/MVA:H/MSC:H/MSI:S/MSA:H/CR:M/IR:H/AR:M/E:P |

**Variation 3: CVSS v4 Score: B+E 8.7**

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | The attacker can execute the exploit with no specific difficulty. No attack requirements are present. |
| Privileges Required | None | The attacker must require privileges sufficient to access the device. |

| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
|---|---|---|
| Vulnerable System Confidentiality | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |
| Vulnerable System Integrity | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |
| Vulnerable System Availability | High | Exploitation of the vulnerability results in complete control of the vulnerable system. |
| Subsequent System Confidentiality | High | The attacker could impact the confidentiality of connected OT devices. |
| Subsequent System Integrity | High | The attacker could impact the confidentiality of connected OT devices. |
| Subsequent System Availability | High | The attacker could impact the confidentiality of connected OT devices. |
| Modified Attack Vector | Network | The system is connected to the Internet for maintenance and services by the robot's suppliers. |
| Modified Attack Complexity | High | There are FW and Data Diodes that prevent access to the PLC. |
| Modified Attack Requirements | None | Same as Base. |
| Modified Privileges Required | Low | Same as Base. |
| Modified User Interaction | None | Same as Base. |
| Modified Vulnerable System Confidentiality | High | The attacker could recover highly valuable information regarding production line data. |
| Modified Vulnerable System Integrity | High | The attacker could modify the operation of the PLC. |
| Modified Vulnerable System Availability | High | The attacker could cause the PLC to stop responding. |
| Modified Subsequent System | High | Potential loss of production data from the connected robotic device. |

| | | |
|---|---|---|
| Confidentiality | | |
| Modified Subsequent System Integrity | Safety | Improper operation of robotic devices could impact the safety of nearby personnel. |
| Modified Subsequent System Availability | High | Equipment failure could result in line downtime. |
| Confidentiality Requirements | Medium | The line contains valuable information. |
| Integrity Requirements | High | Impact to functionality could risk damage to facility and personnel. |
| Availability Requirements | Medium | Although the line should be operational at all times, there is no risk to operators in event of loss of availability. |

# IOT - Healthcare (**CVE-2020-10627**)

Description:

Insulet Omnipod Insulin Management System insulin pump product ID 19191 and 40160 is designed to communicate using a wireless RF with an Insulet manufactured Personal Diabetes Manager device. This wireless RF communication protocol does not properly implement authentication or authorization. An attacker with access to one of the affected insulin pump models may be able to modify and/or intercept data. This vulnerability could also allow attackers to change pump settings and control insulin delivery.

| | **v3.1** | **v4.0** |
|---|---|---|
| **Base** | 8.1<br>CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N | 8.6<br>CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/S:P |
| **Base + Environmental** | | 9.7<br>CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/MSI:S/S:P |

## CVSS v4 Score: Base + Environmental 9.7

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Adjacent | An attacker must be within the local proximity of the device. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No attack requirements are present. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | High | An attacker could exploit the vulnerability to intercept critical data. |
| Vulnerable System Integrity | High | An attacker could exploit the vulnerability to change pump settings and control insulin delivery. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |
| Subsequent System Availability | None | There is no impact to subsequent systems. |
| Exploit Maturity | Unreported | There is no known proof-of-concept code or malicious exploitation of this vulnerability. |
| Modified Subsequent System | Safety | Because control of insulin delivery can be changed, there is a health and human safety impact. |
| Safety | Present | Impact on health and human safety from a vulnerability in an OT device may meet definition of IEC 61508 consequence category **critical**. |

# Value Density (**CVE-2020-28196**)

Description:

MIT Kerberos 5 (aka krb5) before 1.17.2 and 1.18.x before 1.18.3 allows unbounded recursion via an ASN.1-encoded Kerberos message because the lib/krb5/asn.1/asn1_encode.c support for BER indefinite lengths lacks a recursion limit.

|  | v3.1 | v4.0 Base |
|---|---|---|
| **Base** | 7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H | 8.7 CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/V:C |

## CVSS v4 Score: Base 8.7

| Metric | Value | Comments |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | None | No attack requirements are present. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | None | There is no impact to the vulnerable system confidentiality. |
| Vulnerable System Integrity | None | There is no impact to the vulnerable system integrity. |
| Vulnerable System Availability | High | An attacker could cause the application to fail and restart, resulting in a denial of service condition. |
| Subsequent System Confidentiality | None | There is no impact to subsequent systems. |
| Subsequent System Integrity | None | There is no impact to subsequent systems. |

| Subsequent System Availability | None | There is no impact to subsequent systems. |
|---|---|---|
| Value Density | Concentrated | The value of the Kerberos system is highly concentrated due to its functionality in the network environment. |

## Management System (**CVE-2023-20048**)

Description:

A vulnerability in the web services interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute certain unauthorized configuration commands on a Firepower Threat Defense (FTD) device that is managed by the FMC Software.

This vulnerability is due to insufficient authorization of configuration commands that are sent through the web service interface. An attacker could exploit this vulnerability by authenticating to the FMC web services interface and sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to execute certain configuration commands on the targeted FTD device. To successfully exploit this vulnerability, an attacker would need valid credentials on the FMC Software.

Notes:

The vulnerable system is the Firepower Management Center. The subsequent systems are devices managed by the FMC, such as FTD devices. Vulnerability impacts are then limited only to systems managed by the FMC. For the resulting CVSS metrics, there are only subsequent system impacts. There are no additional impacts on the vulnerable system.

|  | **v3.1** | **v4.0 Base** | **v4.0 BTE** |
|---|---|---|---|
| **Base** | 9.9 CVSS:3.1/AV:N/AC:L/PR:L /UI:N/S:C/C:H/I:L/A:H | 6.4 CVSS:4.0/AV:N/AC:L/AT:N /PR:L/UI:N/VC:N/VI:N/VA: N/SC:H/SI:L/SA:H | 2.4 CVSS:4.0/AV:N/AC:L/AT:N /PR:L/UI:N/VC:N/VI:N/VA: N/SC:H/SI:L/SA:H/E:U/M AV:A/R:U/V:C |

**CVSS v4 Score: Base 6.4**

| **Metric** | **Value** | **Comments** |
|---|---|---|

| | | |
|---|---|---|
| Attack Vector | Network | The vulnerable system is accessible from remote networks. |
| Attack Complexity | Low | No specialized conditions or advanced knowledge are required. |
| Attack Requirements | None | No attack requirements are present. |
| Privileges Required | Low | An attacker must have privileges sufficient to log in to the application web-based management interface. |
| User Interaction | None | No user interaction is required for an attacker to successfully exploit the vulnerability. |
| Vulnerable System Confidentiality | None | There is no impact to the vulnerable system confidentiality. An attacker would gain no additional privileges on the vulnerable system as a result of exploitation. |
| Vulnerable System Integrity | None | There is no impact to the vulnerable system integrity. An attacker would gain no additional privileges on the vulnerable system as a result of exploitation. |
| Vulnerable System Availability | None | There is no impact to the vulnerable system availability. An attacker would gain no additional privileges on the vulnerable system as a result of exploitation. |
| Subsequent System Confidentiality | High | An attacker could execute arbitrary commands on the managed devices and gain access to sensitive information. |
| Subsequent System Integrity | Low | An attacker could execute arbitrary commands on the managed devices and change files or modify the configuration. |
| Subsequent System Availability | High | An attacker could execute arbitrary commands on the managed devices and turn off or disable the device. |

## CVSS v4 Score: BTE 2.4

The following threat and environmental metrics further enrich the Management System CVE-2023-20048 example. The scoring scenario shows a Threat metric value of Unreported, and the Modified Attack Vector modified to Adjacent. In this scenario, network-based access controls restrict access to the affected system, changing the expected attack vector for vulnerable systems in this environment.

Additional Supplemental Metrics are chosen to provide more context to the nature of the vulnerability and the affected product, given the importance of the device in most environments.

Refer as well to the full CVSS BTE vector string above.

| Metric | Value | Comments |
|---|---|---|
| Threat | Unreported | No known public exploit exists. |
| Modified Attack Vector | Adjacent | The vulnerable system is not accessible from remote networks. The system is protected by network access control and access is restricted only to trusted hosts. |
| Recovery | User | An exploited device does not recover on its own, and an administrator must reconfigure and recover impacted devices manually. |
| Value Density | Concentrated | An attacker who could exploit this vulnerability could gain control over managed devices that serve as network filtering devices. |

# Version History

| Date | Ver | Description |
|---|---|---|
| 2023-08-10 | v0.1 | Initial Publication |
| 2023-09-29 | v0.2 | Grammatical editing changes, updated metrics score comments, and corrected metric score mismatches. Updated CVE-2021-44228 |
| 2023-10-30 | v0.3 | Added new examples for Value Density (CVE-2020-28196) and Safety (CVE-2023-30560). Additional error corrections |
| 2023-11-01 | v1.0 | Official Release |
| 2024-02-01 | v1.1 | Error corrections in CVE-2020-3549 and CVE-2013-6014. Additional examples for CVE-2022-47379 OT and CVE-2023-20245 ACL bypass. |
| 2024-07-13 | v1.2 | Additional example for subsequent system (CVE-2023-20048)<br>Additional example for SSRF (CVE-2024-1233)<br>Additional example for CSRF (CVE-2023-5602), see accompanying entry |

| | | | in FAQ<br>Additional example, regreSSHion (CVE-2024-6387) |
|---|---|---|---|
| 2024-12-12 | v1.3 | | Additional example for subsequent system (CVE-2023-48228)<br>Included more detailed descriptions for metric choices to describe vulnerable and subsequent systems (CVE-2020-3947)<br>Corrected examples for subsequent system (CVE-2016-5729, CVE-2015-2890, CVE-2018-3652, CVE-2021-44228) |
| 2025-03-14 | v1.4 | | Including new section for CISA KEV example, currently CVE-2025-24201. Adding variation example for XSS to show evaluation for vulnerable system impact (CVE-2022-24682). Additional XSS example for vulnerable system impact (CVE-2024-55228). Error correction on v4.0 Base score for CVE-2021-44228. Updating examples to include variations for Threat and Environmental metrics for CVE-2023-20245 and CVE-2023-20048 |

## (Authors Reference)

## End of Document Notes / Terms

Boilerplate values for None/Low metrics

Attack Complexity: Low
No specialized conditions or advanced knowledge are required.

No built-in security-enhancing conditions exist within the product to inhibit successful exploitation.

Attack Requirements: None
No attack requirements are present.

Privileges Required: None
No privileges are required for an attacker to successfully exploit the vulnerability.

User Interaction: None
No user interaction is required for an attacker to successfully exploit the vulnerability.

Vulnerable system impact: None
There is no impact to the vulnerable system *metric*.
e.g.
There is no impact to the vulnerable system confidentiality.
There is no impact to the vulnerable system integrity.
There is no impact to the vulnerable system availability.

Subsequent system impact: None
There is no impact to subsequent systems.

Exploit Maturity:
Unreported - There is no known proof-of-concept or malicious exploitation of this vulnerability.

| V3.1 | v4.0 |
|---|---|
| Number | Number |
| String | String |