# New Common Vulnerability Scoring System (CVSS) set to be cyber sector game-changer

*The latest tool will be critical to properly assess and prioritize dealing with vulnerabilities and prepare defences against cyber-attacks*

*Critical CVSS 4.0 will also allow consumers to assess real-time threat*

**July 13, 2023** – FIRST has unveiled the latest version of its Common Vulnerability Scoring System (CVSS 4.0).

Last month (June 2023) attendees at the 35th Annual FIRST Conference, in Montréal. Canada got a first-look preview of the new system, with trial usage and sector feedback now underway before its public launch later this year.

Critical in the interface between supplier and consumer, CVSS provides a way to capture the principal characteristics of a security vulnerability and produces a numerical score reflecting its technical severity to inform and provide guidance to businesses, service providers, government, and the public.

The numerical score can be represented as a qualitative severity rating (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes and prepare defences against cyber-attacks.

Furthermore, this system allows the consumer to also assess real-time threat and impact, arming them with vital information to help to defend themselves against an attack.

The Common Vulnerability Scoring System is a published standard used by organizations worldwide, and this latest version of CVSS 4.0 seeks to provide the highest fidelity of vulnerability assessment for both industry and the public.

The programme offers finer granularity in base metrics for consumers, removes downstream scoring ambiguity, simplifies threat metrics, and enhances the effectiveness of assessing environment-specific security requirements as well as compensating controls. In addition, several supplemental attributes for vulnerability assessment have been added including Automatable, Recovery, Value Density, Vulnerability Response Effort and Provider Urgency. There is also additional applicability to OT/ICS/IoT, with Safety metrics and values added to both the Supplemental and Environmental metric groups.

Many leading experts are already testing the new CVSS 4.0, using the new calculator to assess threat levels in their organizations.

This is a significant development for cyber security and incident response teams world-wide. With increasing threats this new CVSS 4.0 is set to be a game-changer for the sector.

Prior to 2005, custom, incompatible rating systems were used to define severity before a need to standardised vulnerability measurements across software and platforms was identified. CVSS version 1 was released in February 2005, developed then by a small group of pioneers with the aim of industry-wide adoption, with FIRST appointed that April to drive the future development of what would become a critical tool in the sector’s arsenal.

Over a dozen FIRST members of the CVSS Special Interest Group (SIG) collaborated extensively through 2006 and 2007 to revise and improve CVSS version 1 by testing and re-testing hundreds of real-world vulnerabilities releasing version 2 in June 2007.

A third version developed the tool further in 2015 introducing the concept of ‘Scope’ in to handle the scoring of vulnerabilities that exist in one software component, but impact a separate software, hardware, or networking component.

Finally, a version 3.1 was released in June 2019 which clarified and improved upon version 3.0 without introducing new metrics or values, improving upon clarity of concepts to improve the overall ease of use of the standard and adding the CVSS Extensions Framework.

However, this latest release marks a significant step forward with added capabilities crucial for teams with the importance of using threat intelligence and environmental metrics for accurate scoring at its core.

Another function of note is the nomenclature. CVSS is not just the Base Score so to further highlight this new nomenclature has been adopted in version 4.0:

- CVSS-B: CVSS Base Score
- CVSS-BT: CVSS Base + Threat Score
- CVSS-BE: CVSS Base + Environmental Score
- CVSS-BTE: CVSS Base + Threat + Environmental Score

Many of the 900 industry leaders, from across the globe, at 35th FIRST annual conference are now testing CVSS version 4.0 in real-time before public launch.

As cyber security issues continue to rapidly increase worldwide global coordination is never more vital to make the internet safe for everyone, and the creation of programs like CVSS 4.0 are essential for both the sector and the public.

Chris Gibson, CEO, FIRST commented: "The CVSS system has rapidly developed over the past 18 years, with each version building on our capabilities to defend from cyber criminality.

"I am immensely proud of the CVSS-SIG for the hard work and dedication it has taken to produce version 4.0. And it is timely as we continue to see a significant rise in threats across the world.

"As a membership organization, our goal is to empower our members and the sector, demonstrating leadership and ensuring we are dedicated to continuously improving how we work together to defend people across the globe against cyber-attacks."

More can be found here https://www.first.org/cvss/

## ENDS

**Issued on behalf of FIRST.**

**For further information please contact:** Paula Mc Nulty

+44 (0)7710 785543 / paula.mcnulty@tigerbond.com.

## ABOUT FIRST:

FIRST aspires to bring together incident response and security teams from every country across the world to ensure a safe internet for all. Founded in 1990, the Forum of Incident Response and Security Teams (FIRST) consists of internet emergency response teams from over 600 corporations, government bodies, universities and other institutions across 100 countries in the Americas, Asia, Europe, Africa, and Oceania.

For more information, visit: https://www.first.org.