New Version of CSAF Standard Provides Vulnerability Exploitability Exchange and Enhances Security for SBOMs Ecosystem

Governments and Companies from Around the World Collaborate to Advance OASIS Open Standard for Automated Security Advisories

BOSTON, MA, USA, November 21, 2022 /EINPresswire.com/ -- OASIS Open, the international open source and standards consortium, announced the approval of the Common Security Advisory Framework (CSAF) 2.0 as a full OASIS standard, a status that signifies the highest level of ratification. This new version of CSAF includes support for the Vulnerability Exploitability Exchange (VEX) profile, which is especially helpful in efficiently consuming SBOM data.

The current threat landscape has profoundly changed how systems and people are protected, driving new approaches to cybersecurity, especially around vendor advisories dealing with vulnerability disclosure issues. The OASIS CSAF Technical Committee's work developing machine readable security advisories makes it possible for cyber defenders to quickly and automatically assess the impact of vulnerabilities and respond in an automated way.

"Security advisories play a crucial role in securing on-premises and cloud-based assets as they contain critical information about how to remediate vulnerabilities," said OASIS CSAF chair, Omar Santos, of Cisco. "CSAF v2.0 brings more than machine readable advisories in JSON format; it specifies the distribution mechanism and how new CSAF documents can be discovered and disclosed. It's the result of an international, industry-wide effort to standardize the reporting of security issues. CSAF enables software producers and consumers to modernize their vulnerability management and response programs."

Sponsor members of the CSAF TC are Accenture, Cisco, Cryptsoft, Cybeats, Dell, EclecticIQ, Hitachi, Huawei, IBM, Microsoft, U.S. NIST, Oracle, and Red Hat. Participation in the OASIS CSAF TC is open to all through membership in OASIS. Providers of products and services that produce, consume, or process security vulnerability remediation information, along with their customers who consume this information, and all other interested parties, are invited to join the group.

The CSAF TC is holding a webinar on Thursday, 1 December at 11am ET, "Using CSAF to Respond

to Supply Chain Vulnerabilities at Large Scale." Speakers include Diane Morris of Cisco, Justin Murphy of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Omar Santos of Cisco, and Thomas Schmidt of the Federal Office for Information Security Germany (BSI). Attendance is free and open to all. View more specifics here.

Support for CSAF

Cybeats
"As the number of vulnerabilities exponentially increases, it is paramount to modernize and automate the way organizations exchange information about these risks. Cybeats is proud to be part of OASIS Open and supports the important work of developing CSAF 2.0, as standard of machine readable format. Cybeats is among the first companies to use CSAF 2.0 to generate VEX for SBOMs."
- Dmitry Raidman, CTO, Cybeats

Oracle
"Oracle is an early adopter of the Common Security Advisory Framework (CSAF) 2.0, an evolution of the Common Vulnerability Reporting Framework (CVRF). CSAF 2.0 further enhances organizations' capabilities in assessing vulnerabilities to prioritize their patching effort. This new version will support the Vulnerability Exploitability eXchange (VEX) format, which provides a means to determine whether specific vulnerabilities in commonly-used components are exploitable in the context of a given product distribution."
- Mary Ann Davidson, Chief Security Officer, Oracle

Red Hat
"Enhancing the security of software supply chains is critical for modern organizations, as complex, multi-footprint digital services take a greater presence in all aspects of society. As a contributor to the CSAF v2.0 framework, we see this effort helping IT security teams to more rapidly and efficiently respond to potential threats via these concepts that modernize and automate security workflows without compromising operations."
- Pete Allor, Director, Red Hat Product Security

About OASIS:
One of the most respected, nonprofit open source and open standards bodies in the world, OASIS advances the fair, transparent development of open source software and standards through the power of global collaboration and community. OASIS is the home for worldwide standards in IoT, cybersecurity, blockchain, privacy, cryptography, cloud computing, urban mobility, emergency management, and other content technologies. Many OASIS standards go on to be ratified by de jure bodies and referenced in international policies and government procurement. https://www.oasis-open.org/

Media inquiries:
communications@oasis-open.org

Carol Geyer
OASIS
+1 941-284-0403
email us here