OASIS Common Security Advisory Framework v2.0 Approved as an ISO/IEC International Standard

Designation as ISO/IEC 20153 Solidifies CSAF's Global Role in Standardized Vulnerability Reporting

BOSTON, MA, UNITED STATES, May 20, 2025 /EINPresswire.com/ -- The Common Security Advisory Framework (CSAF) Version 2.0, an open standard developed by OASIS Open, has officially been approved for release by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Now designated as 'ISO/IEC 20153,' the framework was successfully balloted through the Joint Technical Committee on Information Technology (JTC 1), marking a significant step forward in global security advisory standardization.

"Congratulations to OASIS on the publication of ISO/IEC 20153," said Philip Wennblom, Chair of ISO/IEC JTC 1. "OASIS has been a valued JTC 1 partner since 2004, and this milestone highlights the strength of our collaboration in addressing critical challenges, including in cybersecurity, and advancing standards that benefit consumers, industries, and governments worldwide."

Developed by the OASIS CSAF Technical Committee (TC) through a collaborative, cross-industry effort, CSAF v2.0 provides a modern, machine-readable framework for enhancing vulnerability reporting and response. With support for the Vulnerability Exploitability Exchange (VEX) profile, CSAF v2.0 seamlessly integrates with Software Bill of Materials (SBOM) data, allowing organizations to efficiently assess vulnerabilities and take informed actions.

"Achieving ISO/IEC recognition for CSAF 2.0 is a tremendous milestone for the global cybersecurity community," said Omar Santos, co-chair of the OASIS CSAF TC. "This international standardization will drive broader, more consistent adoption of machine-readable vulnerability disclosures and response processes—ultimately helping organizations around the world protect their assets more effectively and streamline their cybersecurity practices. Whether vulnerabilities emerge in legacy environments or in cutting-edge AI solutions, CSAF 2.0 provides a modern

framework for effective vulnerability reporting in hardware and software. We look forward to continuing our work within the OASIS CSAF TC to ensure the standard remains at the forefront of global cybersecurity efforts."

"CISA is pleased that CSAF 2.0 is now recognized as an ISO/IEC standard, a significant achievement in strengthening global cybersecurity resilience. We value our work and ongoing partnership with OASIS," said Justin Murphy, CISA Vulnerability Disclosure Analyst and co-chair of the OASIS CSAF TC. "CSAF 2.0 enables organizations to respond more effectively to evolving cyber threats across complex environments including critical infrastructure. We encourage and look forward to broader, global adoption of machine-readable standards for vulnerability management efforts."

CSAF v2.0 was ratified as an OASIS Open Standard in November 2022 and subsequently submitted by OASIS to the ISO/IEC JTC 1 Information Technology body. As ISO/IEC 20153, this International Standard will continue to be maintained and advanced by the OASIS CSAF Technical Committee, which includes representatives of Cisco, Cryptsoft, Cyware, Huawei, Microsoft, Oracle, Red Hat, and others. New members are welcome, and participation in the CSAF TC is open to all through membership in OASIS.

About ISO/IEC JTC 1
ISO-IEC Joint Technical Committee (JTC 1) is a consensus based, voluntary international standards group focusing on information technology (IT). Many hundreds of experts from over 100 countries, represent their nation's national standards body or national standards committee to mutually develop beneficial guidelines that enhance global trade, while protecting intellectual property. As one of the largest and most prolific technical committees in the international standardization community, ISO/IEC JTC 1 has had direct responsibility for the development of more than 3,500 published ISO standards, with nearly 600 currently under development. Its work in standardization also encompasses 24 subcommittees that make a tremendous impact on the global ICT industry.

About OASIS Open
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 AI, emergency management, identity, IoT, cybersecurity, blockchain, privacy, cryptography, cloud computing, urban mobility, and other content technologies. Many OASIS standards go on to be ratified by de jure bodies and referenced in international policies and government procurement.
www.oasis-open.org

Media Inquiries: communications@oasis-open.org

Support for CSAF

Cyware:
“Cyware is committed to advancing security automation through the adoption of open, machine-readable standards like CSAF. Integrating CSAF into our threat intelligence and security orchestration platforms enables real-time ingestion, normalization, and automated dissemination of vulnerability advisories, enhancing our customers’ ability to rapidly correlate threat data and initiate timely response actions.”
– Avkash Kathiriya, Sr. VP, Research and Innovation, Cyware Labs

Microsoft:
"The designation of the Common Security Advisory Framework (CSAF) as an ISO/IEC 20153 standard marks a significant milestone for the global vulnerability management ecosystem. At Microsoft, we are proud to support this advancement by publishing advisories conforming to the CSAF specification and expanding its adoption across our security practices. CSAF enhances automation, improves interoperability, and accelerates vulnerability response—empowering organizations worldwide to better protect their ecosystems."
– Bret Arsenault, Corporate Vice President and Chief Cybersecurity Advisor, Microsoft

Disclaimer: CISA does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked or referenced within this press release. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.

Jane Harnad
OASIS Open
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X
