Published on *OASIS* (https://www.oasis-open.org)

OASIS Advances Standard for Automated Disclosure of Cybersecurity Vulnerability Issues

Cisco, EclecticIQ, FireEye, Hitachi, IBM, Intel, LookingGlass, NIST, NC4, Oracle, Red Hat, SafeNet, TELUS, VeriSign, Center for Internet Security, CERT/CC, US DHS, and Others Define Common Security Advisory Framework (CSAF)

17 January 2017 ? Technology providers and their customers are joining forces to advance a standard format for vendors to disclose cybersecurity vulnerabilities. The work of the new OASIS Common Security Advisory Framework (CSAF) Technical Committee will enable greater interoperability among products and ensure that structured, machine-readable security advisories can be produced and consumed much more broadly.

"Defenders need to be able to quickly and automatically assess the impact of a security vulnerability on any of the products they have deployed. We need to get beyond just disclosing vulnerabilities and make it possible to consume and respond to disclosures in an automated way, without the need for special semantic handling of each source," said Art Manion, a Technical Manager of the CERT/CC at the Carnegie Mellon University Software Engineering Institute.

"No software or hardware is immune to security vulnerabilities," said Omar Santos of Cisco, chair of the OASIS CSAF Technical Committee. "Our goal with CSAF is to make it easier for administrators to identify and address known vulnerabilities within their networks, regardless of the platforms they?re using."

CSAF builds on the Common Vulnerability Reporting Framework (CVRF) which was initiated by ICASI, the Industry Consortium for Advancement of Security on the Internet. Several technology vendors (including major Internet backbone providers) already produce advisories in the CVRF format, and many organizations successfully consume this information. ICASI has contributed CVRF 1.1 to the OASIS CSAF Technical Committee for further development.

"We deeply appreciate ICASI bringing this work to OASIS," said Laurent Liscia, CEO and executive director of OASIS. "It?s a natural fit for us. CSAF works with STIX, TAXII, and CybOX, which are cornerstones of the OASIS cybersecurity portfolio. Many members of the OASIS Cyber Threat Intelligence (CTI) Technical Committee are also involved in CSAF."

Support for CSAF

Cisco Product Security Incident Response Team (PSIRT) Director, Klee Michaelis, said, "Machine readable security advisories help security practitioners manage all the disclosures that may affect their organization, efficiently identify and assess affected systems, and more rapidly determine how to remediate security vulnerabilities."

EclecticIQ CEO & Founder, Joep Gommers, said, "The new Common Security Advisory Framework standard

is welcomed as developing standards is of paramount importance in the fight against advanced cyber adversaries."

IBM Senior Security Strategist, Peter Allor, said, "Protecting consumers is the number one priority for security professionals, and industry-wide collaboration requires a common advisory language. CSAF is the evolution of industry efforts to streamline and standardize reporting of accurate and actionable security issues. IBM has been and will continue to be an active participant in the development of security standards."

LookingGlass Cyber Solutions CTO, Allan Thomson, said, "Timely and low-false positive vulnerability and threat intelligence is critical to successfully responding to threats. As a founding member of CASF, LookingGlass is a strong advocate and support of industry efforts to standardize machine-readable vulnerability information. In practice, we have seen that combining vulnerability intelligence with threat intelligence significantly increases an organization?s ability to operationalize their security defenses against an increasingly sophisticated adversary."

NC4 Soltra Development Manager, Mark Davidson, said, "The Common Vulnerability Reporting Framework has enabled the exchange of vulnerability reports for over five years. Moving to OASIS ensures that CSAF and its predecessor, CVRF, will have enduring value. CSAF is poised to help shift costs back toward cyber adversaries, a goal that is in desperate need of achievement. I look forward to the CSAF TC?s success."

Oracle Chief Security Officer, Mary Ann Davidson, said, "Oracle has been an early adopter of CVRF. The adoption of the standard by OASIS, and its promotion as CSAF, will help ensure a wider adoption not only by security companies, but also by customers, who will be in a better position to systematically assess vulnerabilities and prioritize their patching effort. CSAF will be particularly valuable in helping deal with the growing number of vulnerabilities discovered in widely-used open source components."

About OASIS
OASIS is a non-profit, international consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for security, privacy, cloud computing, IoT, SmartGrid, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology. OASIS members broadly represent the marketplace of public and private sector technology leaders, users, and influencers. The consortium has more than 5,000 participants representing over 600 organizations and individual members in 65+ countries. http://www.oasis-open.org

# # #

Press contact: Carol Geyer, carol.geyer@oasis-open.org +1.941.284.0403