Application Vulnerability Description Language (AVDL) Ratified as OASIS Standard

Security Vulnerabilities for Web Services and Web Applications Addressed by New Standard

Boston, MA, USA; 23 June 2004 -- The OASIS international standards consortium today announced that its members have approved the Application Vulnerability Description Language (AVDL) version 1.0 as an OASIS Standard, a status that signifies the highest level of ratification. AVDL provides a standard method for exchanging information concerning security vulnerabilities within Web services and Web applications.

"AVDL addresses the challenge of how businesses manage ongoing application security risk on a day-to-day basis," explained Gartner VP and analyst John Pescatore. "When you consider that upwards of 80 application vulnerabilities are announced each week, it's clear how significant this work is. By employing solutions based on the AVDL OASIS Standard, companies can reduce the threat they face from the moment a vulnerability is discovered to the time it takes them to first shield, then patch their systems."

AVDL is already being implemented by companies and government agencies including the central security incident response organization for the United States Department of Energy (DOE) and National Nuclear Security Administration (NNSA), which plans to AVDL-enable its new Security Incident Response Portal.

"Prior to AVDL, network managers had to manually compare reports from application vulnerability assessments with their application firewall rules, patch management systems, and other information from event correlation engines. Then, they needed to take appropriate remediation steps and create firewall rules to secure their applications," said Kevin Heineman of SPI Dynamics, co-chair of the OASIS AVDL Technical Committee. "Now network managers can save valuable time by importing vulnerability assessment data from AVDL-compliant application scanners. Firewalls can configure appropriate rules, patch management software can provide automatic remediation, and event correlation products can include application-level vulnerability data in the organization's overall risk assessment picture. AVDL offers a welcome alternative to the labor-intensive job of eyeballing and rewriting scores of text alerts, freeing security administrators to focus on higher-level policy analysis."

Jan Bialkowski of NetContinuum, co-chair of the OASIS AVDL Technical Committee, agreed, "Organizations are drowning in the flood of security bulletins and alerts while application vulnerability exploits are wreaking havoc on networks around the globe. AVDL offers an automated way to break this cycle by dramatically reducing the time between the discovery of a new vulnerability and the response time to block attacks at the security gateway. Since AVDL is an easy schema to implement, we hope to see rapid adoption, advancing the industry to an era where all security products can share and effectively utilize vulnerability data via AVDL."

Participation in the OASIS AVDL Technical Committee remains open to all organizations and individuals, and OASIS hosts an open mail list for public comment.
Industry Support for AVDL OASIS Standard

"With the ratification of AVDL, we will now have the capability to provide interoperability between industry-leading network and application security technologies and our vulnerability management solutions. Large enterprise and government customers will benefit enormously from the greater flexibility and consistency for implementing security policies with a standard approach to managing vulnerability data," said Carl Banzhof, CTO, Citadel Security Software.

About OASIS

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. Members themselves set the OASIS technical agenda, using a lightweight, open process expressly designed to promote industry consensus and unite disparate efforts. The consortium produces more Web services standards than any other organization along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets. Founded in 1993, OASIS has more than 3,000 participants representing over 600 organizations and individual members in 100 countries. Approved OASIS Standards include CAP, DocBook, DSML, ebXML, SAML, SPML, UDDI, WSRP, WSS, XACML, and XCBF.
http://www.oasis-open.org [1]

Additional information:

OASIS AVDL Technical Committee

Cover Pages: Application Security

Press contact:

Carol Geyer
OASIS Director of Communications
carol.geyer@oasis-open.org [4]
+1.978.667.5115 x290

Links:
[4] mailto:carol.geyer@oasis-open.org