Major companies team on vulnerability rating system

Major companies, including Cisco and Microsoft, are backing a plan to create a severity scoring system for software holes.

Paul Roberts (IDG News Service) | 21 February, 2005 08:07 | 💬 **Comments** | 🇫 Like

Leading IT companies including Cisco Systems, Microsoft and Symantec are promoting a rating system that will standardize the measurement of the severity of software vulnerabilities.

A plan for the new system, called the Common Vulnerability Scoring System (CVSS), was unveiled at the RSA Conference in San Francisco on Thursday. If widely adopted, the new system will provide a common language for describing the seriousness of computer security vulnerabilities and replace different, vendor-specific rating systems, according to a presentation on the system by Mike Schiffman, a researcher at Cisco.

The new scoring system is part of a project by the National Infrastructure Advisory Council to create a global framework for disclosing information about security vulnerabilities. Representatives from across government and industry contributed to the new CVSS proposal, including eBay, Qualys, Internet Security Systems and Mitre.

NIAC is part of the U.S. Department of Homeland Security and is concerned with the security of information systems that support critical infrastructure for areas such as banking, finance, transportation, energy and manufacturing.

CVSS will use standard mathematical equations to calculate the severity of new vulnerabilities based on basic information such as whether a vulnerability can be remotely exploited, or whether an attacker must log in to a vulnerable system before being able to take advantage of a security hole, said Gerhard Eschelbeck of Qualys.

CVSS ratings will also consider timing issues, such as whether an exploit or a software patch for a specific vulnerability is available, and how long it has been available, he said.

The new rating system will be akin to the Common Vulnerabilities and Exposures (CVE) database that is maintained by Mitre and provides standard identifiers and information about software holes. As with CVE, vendors will most likely use CVSS ratings as a common base of reference, but continue to offer their own analysis or threat assessments, Eschelbeck said.

IT security vendors will use the CVSS in their products to evaluate and prioritize software vulnerabilities. Vendors will also be asked to provide ways for customers to enter information about their IT environment, such as the number and type of systems affected, before calculating a final CVSS rating, he said.

For example, a remotely exploitable vulnerability that affects a worker's desktop system might have a different CVSS rating than one that affects a critical payroll or human resources server, Eschelbeck said.

The system will be different from rating systems such as Symantec's ARIS attack scoring system because it will not be used as a warning system for malicious code outbreaks, according to Schiffman's presentation.

CVSS has backing from major IT players and a detailed plan for implementation. However, the system doesn't yet have a home. Organizers are looking for companies or organizations, such as NIAC or Mitre, to host CVSS and provide portals for Internet users and IT vendors to access the information, Eschelbeck said.

Once it has a host and is widely implemented, CVSS will give IT administrators and vendors an easy way to assess the relative risk of software vulnerabilities and to prioritize patching on large networks, he said.

"It used to be that people never patched their systems, and that didn't work. Then the common wisdom was that you had to patch everything, and that wasn't realistic, either," Eschelbeck said.

"The truth is somewhere in the middle of the two, and prioritization is the key to that," he said.

RELATED WHITEPAPERS

- A Question of Continuity: Maximising Email Availability for Your Business
- Forrester Research Paper | Server Virtualisation Security: 90% Process, 10% Technology
- Customer Story: The New Zealand Automobile Association increases response rates and savings with SAS
- Pulling the Plug on Legacy Log Management
- The Pathways ICT Leadership Development Program | Turning today's ICT professionals into tomorrow's business leaders

COMMUNITY COMMENTS

- "@industry observer: You're sprung. 'Fess up, you're really the evil Conboy in ..." on **HP projection technology could take a page from Star Wars**
- "@RS, now look what you've done to poor old Realist. Where are ..." on **Opinion: We need to think in multiples on broadband**
- "Could we filter out Tony Abbott holograms ?" on **HP projection technology could take a page from Star Wars**
- "Speaking of hypocritical to the extreme (and conceitedly so)... From your first ..." on **Opinion: We need to think in multiples on broadband**
- "All of those commentors who believe unlimited is sustainable should put your ..." on **'Unlimited' broadband dead in the water: iiNet, iPrimus**