

Welcome to the latest edition of the CVE-Announce e-newsletter. This email newsletter is designed to bring recent news about CVE, such as new versions, upcoming conferences, new Web site features, etc. right to your mailbox. Common Vulnerabilities and Exposures (CVE) is a list or dictionary that provides common names for publicly known information security vulnerabilities and exposures. CVE content results from the collaborative efforts of the CVE Editorial Board, which is comprised of leading representatives from the information security community. Details on subscribing (and unsubscribing) to the email newsletter are at the end.

Comments: cve@mitre.org

CVE-Announce e-newsletter/May 13, 2004

Contents:

1. Feature Story
2. Hot Topic #1: Compatibility Milestone!
3. Hot Topic #2: Forrester Research Study
4. Latest Compatible Products/Services
5. Upcoming Events
6. Also in this Issue
7. Subscribe to "CVE-Data-Update" for Technical Updates
8. Details/Credits + Subscribing and Unsubscribing

FEATURE STORY:

'OVAL XML Reference Interpreter' Finds Vulnerabilities from the CVE Dictionary

MITRE's Open Vulnerability Assessment Language (OVAL) project has released two free Reference XML Definition Interpreters that can determine if a system has vulnerabilities from the CVE dictionary. MITRE developed the Reference Interpreters to demonstrate the usability of OVAL vulnerability definitions, which are gold-standard tests written by the information security community to provide a standardized baseline check for determining the presence of vulnerabilities on end systems. OVAL definitions are based on CVE names; for each name there are one or more definitions.

A Reference Interpreter for Microsoft Windows supports Windows NT 4.0, 2000, XP, and Server 2003, while another supports Red Hat Linux 9 and Red Hat Enterprise Linux 3. The Interpreters are not fully functional scanning tools and have a simplistic user interface, but running one will provide a list of CVE names determined by OVAL to be present on the system. This list is in a format that can easily be incorporated into other information security tools.

Both Interpreters and their associated data files are available for download for free from the OVAL Web site at <http://oval.mitre.org/oval/download/interpreter.html#download>

LINKS:

OVAL Web site - <http://oval.mitre.org/>

CVE names - http://cve.mitre.org/docs/docs2000/naming_process.html

HOT TOPIC #1:

CVE Compatibility Milestone: 100+ Organizations Now Participating!

As of March 17, 2004, the CVE Initiative achieved a major milestone with 103 organizations from industry, government, and academia around the world now working to make their products or services CVE-compatible. Sixteen countries are represented, with 167 information security products and services declared CVE-compatible or in the process of being made compatible by these organizations. Of the 167, 14 products/services from 10 organizations have achieved the final phase of MITRE's formal CVE Compatibility Process and are now officially CVE-compatible. These are indicated in the CVE-Compatible Products and Services section of this site with the CVE-Compatible product/service logo. (Current numbers are 180 products and services from 111 organizations.)

"CVE-compatible" means that a product or service uses CVE names in a way that allows it to cross-link with other repositories that also use CVE names, as documented in the CVE compatibility requirements. Each item listed on the CVE Web site includes a link to the organization's homepage, the product or service name, type of product, link to the product homepage, and a notation of the specific point in the CVE Compatibility Process each product or service has reached. Many organizations have multiple products and services listed. For additional usability, they are also listed by product type, product name, organization, and country. Product types include vulnerability databases; security archives and advisories; vulnerability assessment and remediation; intrusion detection, management, monitoring, and response; incident management; data and event correlation; educational materials; and firewalls.

Visit the CVE-Compatible Products and Services page to review information about CVE compatibility, and on all 180 information security products and services.

LINKS:

CVE-Compatible Products and Services - <http://cve.mitre.org/compatible/>

CVE Compatibility Process - <http://cve.mitre.org/compatible/process.html>

CVE Compatibility Requirements - <http://cve.mitre.org/compatible/requirements.html>

HOT TOPIC #2:

CVE the Underpinning for Forrester Research Study

CVE was the underpinning for a Forrester Research study that compared Linux versus Windows in terms of how quickly they fixed security vulnerabilities. The study, which was the topic of a March 30, 2004 article in eWeek entitled "Linux vs. Windows: Which Is More Secure?" would not have been feasible without CVE. It is the first time CVE has been used to support such a large-scale, quantitative analysis. The authors used the National Institute of Standards and Technology's (NIST) ICAT database—which NIST describes as a "CVE Vulnerability Search Engine"—to perform the comparison and to normalize their results. The study is available for purchase on the Forrester Web site.

NIST is a member of the CVE Editorial Board and ICAT is listed on the CVE-Compatible Products and Services page.

LINKS:

Forrester Research study -
<http://www.forrester.com/Research/Document/Excerpt/0,7211,33941,00.html>

eWeek article - <http://www.eweek.com/article2/0,1759,1557459,00.asp>

NIST ICAT database - <http://icat.nist.gov/icat.cfm>

CVE-Compatible Products and Services page - <http://cve.mitre.org/compatible/>

LATEST COMPATIBLE PRODUCTS/SERVICES:

- * Beyond Security Ltd. Makes CVE Compatibility Declaration
- * Acrobe Consulting AB Makes CVE Compatibility Declaration
- * Open Source Vulnerability Database (OSVDB) Makes CVE Compatibility Declaration
- * Sourcefire, Inc. Makes CVE Compatibility Declaration

- * Cubico Solutions CC Makes CVE Compatibility Declaration
- * Skybox Security, Inc. Makes CVE Compatibility Declaration
- * NX Security Makes CVE Compatibility Declaration
- * Shavlik Technologies, LLC Makes CVE Compatibility Declaration
- * LURHQ Corporation Makes CVE Compatibility Declaration
- * KaVaDo Inc. Makes CVE Compatibility Declaration
- * GuardedNet, Inc. Makes CVE Compatibility Declaration
- * OpenService, Inc. Makes CVE Compatibility Declaration
- * SecureWorks, Inc. Makes CVE Compatibility Declaration
- * Secure Elements, Incorporated Makes CVE Compatibility Declaration
- * Sandvine Incorporated Makes CVE Compatibility Declaration
- * SECNAP Network Security Corporation Makes CVE Compatibility Declaration
- * Sunbelt Software, Inc. Makes CVE Compatibility Declaration
- * Visionael Corporation Makes CVE Compatibility Declaration

Find more information on these and other products at <http://cve.mitre.org/compatible/>

UPCOMING EVENTS:

June 6-9, 2004

"Sixth Annual International Techno-Security Conference," Myrtle Beach, South Carolina, USA

--OVAL/CVE booth

June 15-16, 2004

"NetSec 2004 Conference & Exhibition," San Francisco, California, USA

--OVAL/CVE booth

Visit the CVE Calendar page for conference URLs and more upcoming events at

<http://cve.mitre.org/news/calendar.html>

ALSO IN THIS ISSUE:

- * CVE Topic of Question in Q&A Article about Red Hat Security Response in "Wide Open Magazine"
- * CVE to Present Briefing at "SecurE-Biz CxO Security Summit" on June 11, 2004
- * CVE and OVAL Included as Chapter in Book on Software Quality Management
- * CVE Included as Chapter in 5th Edition of "Information Security Managers Handbook"
- * CVE Included as a "Best Practice" in Book about E-Business Systems Security
- * CVE Presents Briefing at "16th Annual Systems & Software Technology Conference"
- * OVAL e-Newsletter Includes CVE Names in Each Issue
- * CVE Mentioned in "eWeek" Article about the Launch of the Open Source Vulnerability Database
- * CVE Senior Advisory Council Holds Meeting
- * CVE Presents Briefing at "12th International British Computer Society Conference on Software Quality Management"
- * MITRE Hosts CVE/OVAL Booth at "InfoSec World Conference and Expo/2004," March 22nd-24th
- * Conference Photos of CVE Booth at "RSA 2004," February 23rd-27th
- * Several Organizations Reference CVE Names in Security Advisories

Read these stories and more news at <http://cve.mitre.org/news>

Subscribe to "CVE-Data-Update" for Technical Updates

Intended for technical users of CVE such as vulnerability database maintainers or those who require timely notification of new candidates, the "CVE-Data-Update" e-newsletter

provides subscribers with reports of new CVE entries and/or candidates and other detailed technical information regarding CVE. Subscribe now at <http://cve.mitre.org/signup/register.html>.

Details/Credits + Subscribing and Unsubscribing

Managing Editor: Steve Christey, Information Security Technical Center. Writer: Bob Roberge, Corporate Communications. The MITRE Corporation (www.mitre.org) maintains CVE and provides impartial technical guidance to the CVE Editorial Board on all matters related to ongoing development of CVE.

To unsubscribe from the CVE-Announce e-newsletter, open a new email message and copy the following text to the BODY of the message "SIGNOFF CVE-Announce-list", then send the message to: listserv@lists.mitre.org. To subscribe, send an email message to listserv@lists.mitre.org with the following text in the BODY of the message: "SUBSCRIBE CVE-Announce-List".

Copyright 2004, The MITRE Corporation. CVE and the CVE logo are registered trademarks of The MITRE Corporation.

For more information about CVE, visit the CVE Web site at <http://cve.mitre.org> or send an email to cve@mitre.org.