

Welcome to the inaugural edition of the CWE-Announce e-newsletter. This email newsletter is designed to bring recent news about CWE, such as new versions, new compatible products, upcoming conferences, new Web site features, etc. right to your mailbox. Common Weakness Enumeration (CWE) provides a unified, measurable set of software weaknesses that will enable more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code. Details on subscribing (and unsubscribing) to the email newsletter are at the end.

Please feel free to pass this newsletter on to interested colleagues.

Comments: cwe@mitre.org

CWE-Announce e-newsletter/March 14, 2007

Contents:

1. Feature Story
2. Latest Compatible Products
3. Upcoming Events
4. Also in this Issue
5. Details/Credits + Subscribing and Unsubscribing

FEATURE STORY:

CWE Main Focus of Article in "InfoWorld"

CWE was the main focus of a March 1, 2007 article in "InfoWorld" entitled "Software Vulnerability Index making progress." The article describes what CWE is, the benefits it provides for software developers and acquirers, mentions several of the sources used to create the list, and describes how the final draft of the list is being formed. The article also includes quotes by CWE Program Manager Robert A. Martin on the reason for CWE: "We wanted to evaluate what the tools claim to cover and what they are most effective at finding. Right now, best test is to throw tools at a big pile of code and see what tools find the most vulnerabilities, but we're changing that paradigm [with CWE] into test cases where we now look at the answers so we can evaluate what the tools found and what kinds of complexities they can handle."

The author also paraphrases Martin in describing the creation of the

CWE List: "CWE's research will not list the names and performance results of the products it is testing -- provided by over 20 firms, including Cenzic, Fortify, SPI Dynamics, Veracode, and Watchfire -- but the work to compile a resource that offers developers an idea of the types of vulnerabilities missed by the tools should provide a great deal of value."

Also included is a quote by Sean Barnum, director of knowledge management at Cigital, regarding the CWE research: "We found that less than half of what we already have in CWE is covered by these tools, so this helps prove that there are a lot of known issues out there that aren't being addressed. We also thought that the tools would look for the same types of things, but they are actually very different, and there's not a lot of overlap; that's something that developers need to be aware of as they choose tools; you want to right set for aggregated coverage."

The author closes the article with a description of how the CWE dictionary is being developed: "Before each release of CWE, workers with the project spend much of their time comparing all the vulnerability definitions and mitigation taxonomies in the index, attempting to refine the language used in the descriptions and add real-world examples of attacks that target the flaws. That work is continuing and will remain the primary focus of CWE's efforts going forward ... including work to de-emphasize nomenclature that describes common problems based on the attack methods used to exploit them."

LINKS:

InfoWorld article -

http://www.infoworld.com/article/07/03/01/HNcweprogress_1.html

CWE Web site - <http://cwe.mitre.org>

LATEST COMPATIBLE PRODUCTS:

Three (3) additional organizations have made declarations of CWE Compatibility for five (5) products and services:

* Armorize Technologies, Inc. declared that its Web application source code analysis suite, CodeSecure Verifier, Web application source code analysis tool, CodeSecure Enterprise, and its Web application source

code analysis tool, CodeSecure Workbench, will be CWE-Compatible.

* CERIAS/Purdue University (www.cerias.purdue.edu) declared that its Secure Programming Class and its Publicly Available Teaching Materials for it Materials are CWE-Compatible.

* SofCheck, Inc. (www.sofcheck.com) declared that its static analysis and fault detection tool, SofCheck Inspector for Ada, will be CWE-Compatible.

For additional information about these and other compatible products, visit the CWE Compatibility and Effectiveness section on the CWE Web site. There are now 20 declarations of CWE Compatibility from 10 organizations from around the world.

LINK:

CWE Compatibility and Effectiveness section -
<http://cwe.mitre.org/compatible/index.html>

UPCOMING EVENTS:

CWE is scheduled to participate in two industry events in March:

CWE is scheduled to co-host a Making Security Measurable (<http://measurablesecurity.mitre.org>) exhibitor booth at "InfoSec World 2007 Conference & Expo" on March 19-21, 2007 at the Rosen Shingle Creek Resort in Orlando, Florida, USA. The conference will expose MITRE's CWE (cwe.mitre.org), CVE (cve.mitre.org), CCE (cce.mitre.org), CME (cme.mitre.org), CPE (cpe.mitre.org), and OVAL (oval.mitre.org) efforts to a diverse audience of attendees from the banking, finance, real estate, insurance, and health care industries, among others. The conference is targeted to information security policy and decision makers from these and other industries, as well as directors and managers of information security, CIOs, network and systems security administrators, IT auditors, systems planners and analysts, systems administrators, software and application developers, engineers, systems integrators, strategic planners, and other information security professionals. Organizations with CWE-Compatible Products and Service declarations are also exhibiting.

In addition, CWE is scheduled to present a briefing about CWE on March 26-30, 2007 at the "OMG Software Assurance Special Interest Group" meeting in San Diego, California, USA.

Visit the CWE Calendar page at <http://cwe.mitre.org/news/calendar.html> for information on these and other upcoming events.

LINKS:

"InfoSec World 2007" - <http://www.misti.com/default.asp?page=65&return=70&productid=5539>

"OMG Software Assurance Special Interest Group" - <http://swa.omg.org>

CWE Calendar - <http://cwe.mitre.org/news/calendar.html>

ALSO IN THIS ISSUE:

- * CWE Main Focus of Article in "Computerworld"
- * CWE Main Focus of Article on "ZDNet.com"
- * CWE A Main Topic of Article on "Dark Reading"
- * CWE Hosts Booth at "OMG Software Assurance Workshop," March 5-7
- * CWE Presents Briefing & Participates on Discussion Panel at "DoD/DHS Software Assurance Forum" on March 9
- * CWE Main Topic of Article in "CrossTalk Magazine"
- * CWE Mentioned in Award Description in "2007 SC Magazine Awards"
- * Photos from CWE Booth at "2007 Information Assurance Workshop"

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

Details/Credits + Subscribing and Unsubscribing

Managing Editor: Robert A. Martin. Writer: Bob Roberge. The MITRE Corporation (www.mitre.org) maintains CWE and provides impartial technical guidance to the CWE Community on all matters related to ongoing development of CWE.

To unsubscribe from the CWE-Announce e-newsletter, open a new email message and copy the following text to the BODY of the message "SIGNOFF CWE-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 CWE-Announce-List".

Copyright 2007, The MITRE Corporation. CWE and the CWE logo are registered trademarks of The MITRE Corporation.

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