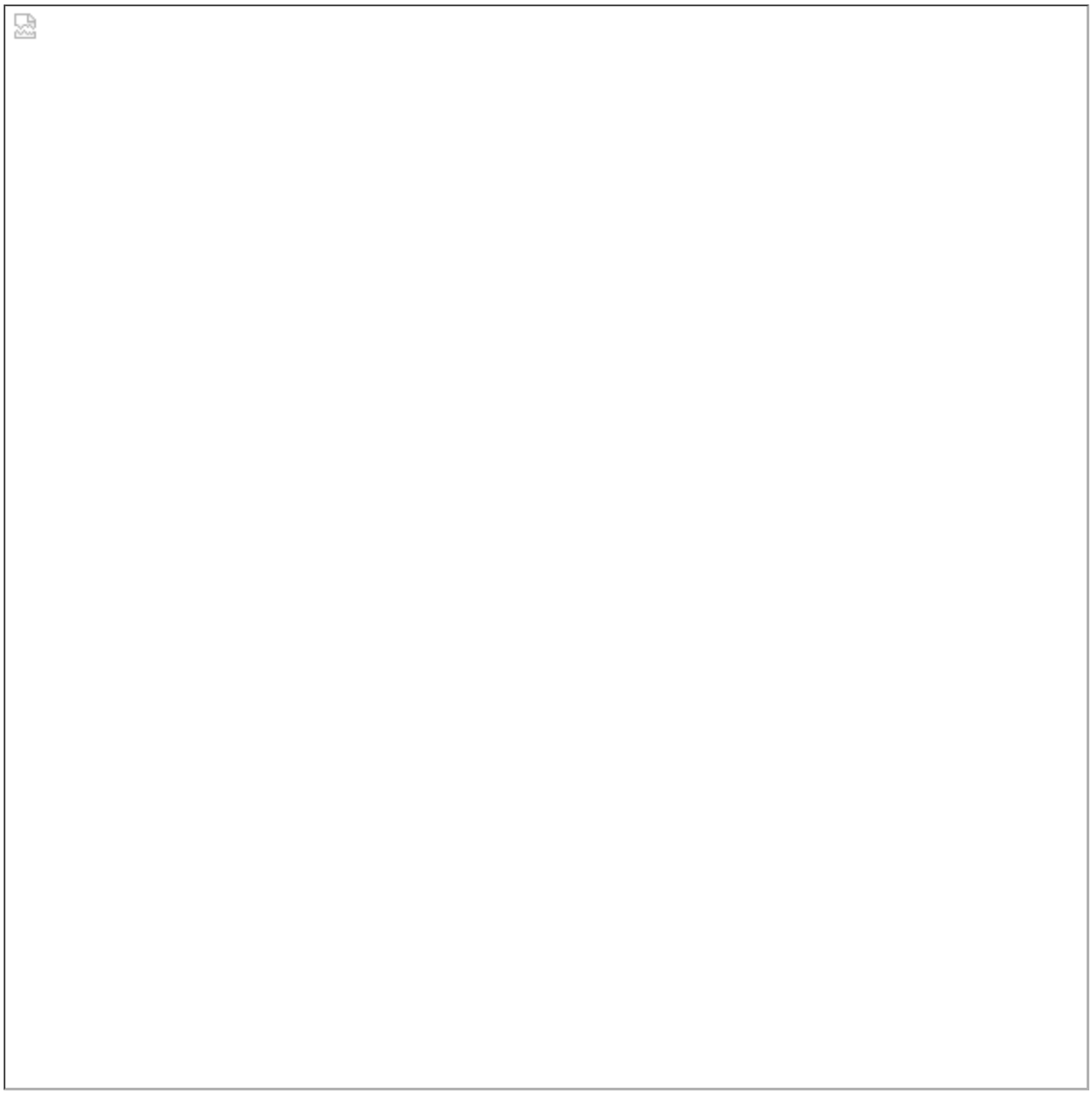

August 2013 Edition

News
Language Standards Updates
Upcoming Events and Training
Our People
Secure Coding Resources

News

This is the second monthly Secure Coding eNewsletter. Our goal is to provide you with timely information concerning updates to the CERT secure coding standards and to make you aware of other interesting news and events related to secure coding. If you wish to unsubscribe, just use the SafeUnsubscribe link at the end of this newsletter.

Normally things slow down in the summer, especially at a university, but the wiki has seen a lot

of activity this past month. In particular, we are working toward updating the CERT C Secure Coding Standard for C11 and as always, we are looking for help. In particular, C11 adds concurrency support to the language so we have much work to do to make sure we cover the security implications of these new features in our coding standard.

Another area that will be seeing increased activity is the development of additional rules for the Android (DRD) appendix. This appendix includes rules that are specific to developing Java apps for the Android platform. Dr. Fred Long has joined us here at CERT for the remainder of the summer and will be working in this area.

In addition to working on secure coding standards for C, C++, Java, and Perl on the public wiki, we have also begun efforts to create secure coding standards for various other languages, including Ada, C#, Fortran, Python, JavaScript, and SPARK. We will share these standards with the public once they move beyond the embarrassing stage. If you would like to contribute to the development of these standards, please contact us at secure-coding@cert.org.

Language Standards Updates

CERT C Secure Coding Standard

Editors: Martin Sebor (Cisco Systems), Aaron Ballman (SEI)

Standards Added

51. Microsoft Windows (WIN) Added a section specific to Microsoft Windows APIs, similar in concept to the existing POSIX section. This area is a work in progress.
MSC41-C. Beware of vendor-specific library and language differences Added a new rule to caution against vendor-specific differences. This rule has an excellent section specific to Microsoft Visual Studio, but could use further efforts for other vendors.
API05-C. Use conformant array parameters New rule to encourage the use of variables in the indices of array parameter declarations. This does not change the semantics of the declarations, but does improve API documentation.

Standards Changed

John Benito from Blue Pilot is working on the threads examples in the CON section, as they are currently incorrect in many ways.

John is also working on a common error handling approach with the goal to remove all of the "/* handle error */ style messages.

FIO03-C. Do not make assumptions about fopen() and file creation Noted that Microsoft Visual Studio 2012 and earlier do not support the 'x' mode character; added a compliant solution for Windows.
FIO11-C. Take care when specifying the mode parameter of fopen() Updated for Annex K, noted that Microsoft Visual Studio 2012 and earlier do not support the 'x' or 'u' mode characters.

Unresolved Issues

EXP35-C is obsolete with the changes to C11, but we are trying to figure out how to retain the guidance for C99 and earlier version of the standard.

There is a conflict between PRE03-C. Prefer typedefs to defines for encoding types and DCL05-C. Use typedefs of non-pointer types only that needs to be resolved. PRE03-C has

a compelling code example that demonstrates the dangers of using macros to define types, but the solution involves using a typedef for a pointer type, which contradicts the recommendation of DCL05-C. Comments, suggestions, or possible solutions are welcome!

No C rules were removed or deprecated last month.

CERT C++ Secure Coding Standard

Editors: Martin Sebor (Cisco Systems), Aaron Ballman (SEI)

No C++ rules were added, removed, deprecated, or substantively changed last month.

CERT Oracle Secure Coding Standard for Java

Editors: Adam O'Brien (Oracle), David Svoboda (SEI)

No Java rules were removed last month.

Standards Added

DRD04-J. Do not log sensitive information

Standards Changed

DRD02-J. Do not allow WebView to access sensitive local resource through file scheme More detailed explanation of the dangerous methods has been provided.

CERT Perl Secure Coding Standard

Editor: David Svoboda (SEI)

No Perl rules were added last month.

Standards Changed

John Benito from Blue Pilot is working on the threads examples in the CON section, as they are currently incorrect in many ways.

John is also working on a common error handling approach with the goal to remove all of the "/* handle error */ style messages.

IDS35-PL. Do not invoke the eval form with a string argument In IDS35-EX0, noted that eval '$x' is indeed string-based evaluation (not block-based evaluation) and hence noncompliant with the rule.
DCL30-PL. Do not import deprecated modules Improved introduction. This rule should maintain a list of modules that the Perl community believe should not be used, for various reasons. The community does not officially categorize them as 'deprecated', but CERT does.

Standards Removed

DCL32-PL. Every module must return a true value This rule is deemed not to be relevant to security, because a module that violates it can not be loaded into a working Perl program.

Upcoming Events and Training

Managing the Insider Threat: What Every Organization Should Know (Virtual Event)
August 8, 2013
Register at www.sei.cmu.edu/goto/managing-the-insider-threat

Members of the Secure Coding Initiative will be giving three presentations at the JavaOne 2013 conference

Session ID: CON6396 Don't Be Pwned: A Very Short Course on Secure Programming in Java presented by Dean Sutherland and Robert Seacord
Session ID: CON3122 Anatomy of a Java Zero-Day Exploit presented by David Svoboda
Session ID: TUT5599 The Java Security Architecture: How and Why presented by David Svoboda

Mini-Track Announcement | Hawaii International Conference on Systems Sciences
Software Security for Mobile Platforms
January 6-9, 2014
Hilton Waikoloa, Big Island, Hawaii

Secure Coding in C and C++ Course
This four-day course provides a detailed explanation of common programming errors in C and C++ and describes how these errors can lead to code that is vulnerable to exploitation. The course concentrates on security issues intrinsic to the C and C++ programming languages and associated libraries. This course may be offered by special arrangement at customer sites. Contact course-info@sei.cmu.edu

Our People

Each month we will highlight staff members behind our secure coding research. This month we feature David Svoboda and Fred Long.

David Svoboda has been the primary developer on a diverse set of software development projects at Carnegie Mellon University since 1991. Hi projects have ranged from hierarchical chip modeling and social organization simulation to automated machine translation (AMT). His KANTOO AMT software, developed in 1996, is still in production use at Caterpillar. He has over 13 years of Java development experience, starting with Java 2, and his Java projects include Tomcat servlets and Eclipse plug-ins. He has taught Secure Coding in C and C++ all over the world to various groups in the military, government, and banking industries.

Fred Long is a senior lecturer and director of learning and teaching in the Department of Computer Science, Aberystwyth University, United Kingdom. He lectures on formal methods; Java, C++, and C programming paradigms and programming-related security issues. He is chairman of the British Computer Society's Mid-Wales Sub-Branch. Fred has been a Visiting Scientist at the Software Engineering Institute since 1992. Recently, his research has involved the investigation of vulnerabilities in Java.

Secure Coding Resources

Watch Robert Seacord discuss the Source Code Analysis Laboratory (SCALe)

Listen to Mary Ann Davidson and Julia Allen discuss Developing Secure Software: Universities as Supply Chain Partners

Read David Svoboda's Blog post: Using the Pointer Ownership Model to Secure Memory Management in C and C++

Subscribe to Our eNewsletter

Join the SEI CERT Secure Coding Community