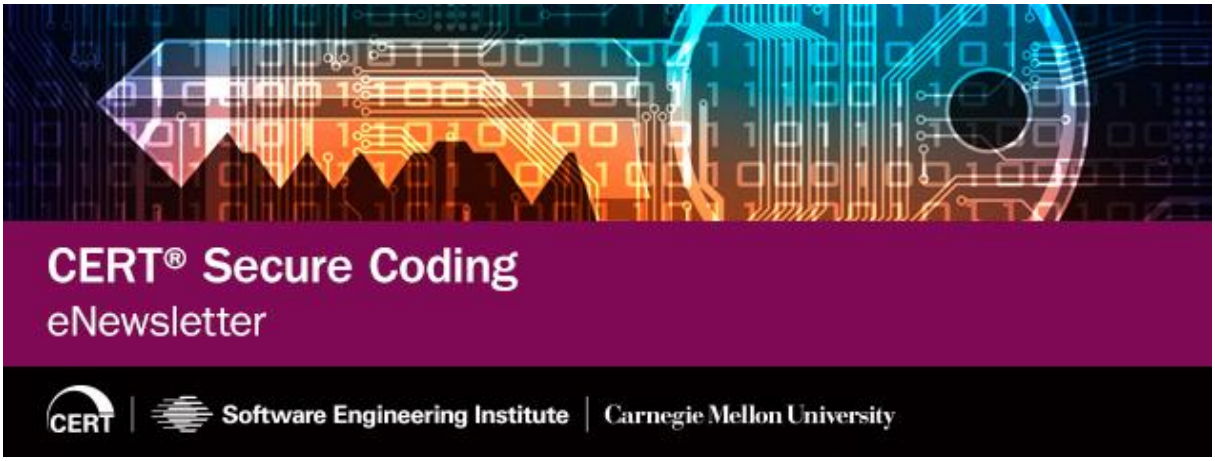
SHARE:

Join Our Email List



Summer Edition 2017

Welcome to the Summer 2017 Edition of the CERT Secure Coding Standards eNewsletter!

We are two-thirds of the way through summer, and it has gone by quickly, as it usually tends to do. So far this summer, we released a few SEI Cyber Minute videos and blog posts, which you can find below. We are also starting to write draft guidelines for Ada and are looking for contributors.

We are planning to grow our team and have several open positions in secure coding and software assurance. If you or someone you know wants to improve the state of the art and practice of secure coding, secure development, or software assurance in general, see the information below about our open positions.

As always, we hope you find the information in this eNewsletter useful. Please email us at info@sei.cmu.edu to let us know your thoughts about our work, or send your comments or ideas about what we should do next.

Looking ahead, a few of us will be at IEEE SecDev in September. I hope to see you at an upcoming event.

Thanks and enjoy the rest of the summer!

Bob Schiela

News

Open Positions in SEI CERT Secure Coding Team

Join our Secure Coding team. If you have the right qualifications and are interested in researching and developing improvements to the state of the art and practice in secure coding, secure development, and software assurance, please consider applying for any of the following positions:

- Senior Software Security Engineer
- Senior Software Assurance Engineer (El Segundo, CA; Aurora, CO; Bedford, MA; Arlington, VA)
- Software Security Analyst
- Compiler Researcher
- Software Engineer

Request for Contributors: Ada Guidelines

We are developing draft guidelines for Ada. If you would like to contribute to these guidelines by providing content or reviewing material, please send us a note at info@sei.cmu.edu.

Mapping Refresh: CERT Guidelines to MITRE CWEs

We are collaborating with MITRE to refresh the mappings between CERT guidelines and MITRE CWEs. Both MITRE and CERT will publish the revised mappings.

Publications

In July, Karan Dwivedi, Hongli Yin, Pranav Bagree, Xiaoxiao Tang, Lori Flynn, William Klieber, and William Snavely published a new SEI technical report titled DidFail: Coverage and Precision Enhancement. This report describes work to enhance DidFail, our Android app set taint flow analyzer.

In June, Christopher Alberts, John Haller, Charles Wallen, and Carol Woody published a CrossTalk journal article titled " Assessing DoD System Acquisition Supply Chain Risk Management." This article presents a framework of supply chain risk management practices to measure and improve an organization's ability to manage third-party cyber risks.

In April, Christopher Alberts and Carol Woody published a new SEI technical note titled Prototype Software Assurance Framework (SAF): Introduction and Overview. In it, Chris and Carol discuss the SAF, a collection of cybersecurity practices that programs can apply across the acquisition lifecycle and supply chain.

We contributed several overviews to the SEI Cyber Minute video series about secure development:

- Automated Code Repair (by Will Klieber)
- Code Flaw Alert Classification (by Lori Flynn)
- Secure Coding Standards (by Robert Schiela)
- Securing Open Source Components (by Mark Sherman)

- Adding Security to Agile's Scrum (by Mark Sherman)

We also published the following blog posts:

- CERT C++ Secure Coding Guidelines (by David Svoboda)
- Three Pilots of the CERT Software Assurance Framework (by Christopher Alberts and Carol Woody)

In June, Mark Sherman recorded the webinar "Building Secure Vehicular Software" on BrightTALK. In the webinar, Mark explores the expanding landscape of vulnerabilities that accompany the increasing reliance on software and examines key steps to help mitigate the increased risk.

Recent Events

Several Secure Coding and Cyber Security Engineering team members made notable presentations and tutorials at the Software Solutions Symposium 2017:

- David Svoboda taught "Secure Coding Tutorial" on March 23, 2017.
- Nancy Mead taught "Eliciting Innovative Requirements for DoD Systems: The KJ+ Method" on March 20, 2017.
- Carol Woody taught "Security Risk Management Using the Security Engineering Risk Analysis (SERA) Method Tutorial" on March 20, 2017.

You can download presentations from the Software Solutions Symposium 2017 collection in the SEI digital library: http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=495735.

Upcoming Events

In September, Lori Flynn, David Svoboda, and William Snavely will present "Hands-On Tutorial: Auditing Static Analysis Alerts Using a Lexicon & Rules" at the IEEE CyberSecurity Development (SecDev) Conference.

SEI CERT Secure Coding Standard Updates

CERT C Coding Standard

Editors: David Svoboda, SEI/CERT

Download the latest stable version.

No C rules were added or removed.

Changed

- *The first noncompliant code example MEM35-C. Allocate sufficient memory for an object now checks for compliance with INT30-C. Ensure that unsigned integer operations do not wrap, not INT32-C. Ensure that operations on signed integers do not result in overflow.*

- *The macros in the code examples in PRE10-C. Wrap multistatement macros in a do-while loop now comply with PRE02-C. Macro replacement lists should be parenthesized and have been documented to be unsafe, as recommended by PRE12-C. Do not define unsafe macros.*

CERT C++ Secure Coding Standard

Editors: David Svoboda, SEI/CERT

Download the latest stable version.

No C++ rules were added.

- *OOP52-CPP. Do not delete a polymorphic object without a virtual destructor has a new exception permitting destruction of derived objects without virtual destructors if the object is not referenced by a base pointer.*

CERT Oracle Secure Coding Standard for Java

Editor: David Svoboda, SEI/CERT

Download the latest stable version.

No Java rules were added or removed.

Changed

- Several changes were made to LCK00-J. Use private final lock objects to synchronize classes that may interact with untrusted code:
    - The attack code in the first noncompliant code example is more practical since the object to lock must be accessible to trusted code.
    - The 'package-private' exception only applies to classes that never get exposed to untrusted code.
    - The attack code that uses `Object.wait()` was removed since it should cause an `IllegalMonitorException` to be thrown.

CERT Secure Coding Standard for Android

Editor: Lori Flynn, SEI/CERT

No Android rules were added, removed, deprecated, or substantively changed.

CERT Perl Secure Coding Standard

Editor: David Svoboda, SEI/CERT

No Perl rules were added or removed.

Our People

In our eNewsletters, we highlight the staff members behind our secure coding research. In this issue we feature Will Snavely.

Will Snavely is an associate software engineer at the CERT Division of the Software Engineering Institute in Pittsburgh, PA. He joined the team in 2015, after graduating from Carnegie Mellon University with a master's in information security. Since then, he has helped develop and maintain SEI CERT Secure Coding Standards and has contributed to exciting research led by Lori Flynn (machine learning classification of static analysis results) and Will Klieber (automated code repair). He has also helped teach secure coding courses with David Svoboda . On his mind lately are the practical aspects of integrating software assurance--especially software security--into a development lifecycle. How does a program decide which software assurance techniques to apply, and how does it measure/assess the benefits of doing so? Will is particularly interested in the application of formal methods to software development. To this end, he has been investigating the Ada language and its derivatives, such as SPARK. Drop Will an email if you want to discuss his work or if you have questions about it.

Subscribe to Our eNewsletter

Join the SEI CERT Secure Coding Community