CERT | Software Engineering Institute Carnegie Mellon University

SEI Insights

CERT/CC Blog

Vulnerability Insights

CERT Basic Fuzzing Framework Update

POSTED ON SEPTEMBER 22, 2010 BY WILL DORMANN [/AUTHOR/WILL-DORMANN] IN TOOLS [HTTPS://INSIGHTS.SEI.CMU.EDU/CERT/TOOLS/]

Hi, folks. We've recently updated the CERT® Basic Fuzzing Framework (BFF). The new BFF 1.1 contains new functionality and improves performance.

The BFF is a framework to perform file mutation fuzzing for Linux applications. Since the initial release of the BFF [http://www.cert.org/blogs/vuls/2010/05/cert_basic_fuzzing_framework.html], we have made some improvements:

The virtual machine

- We upgraded the OS to the testing version of Debian ("Squeeze"). In the process of installing applications to fuzz, I noticed that some of them required libraries newer than what are available in the stable version of Debian. The VM used by the BFF is more modern.
- The virtual machine now includes a generic VESA video driver in addition to the VMware driver. This can simplify the use of the BFF with other virtualization products, like VirtualBox.

The scripts

- In some cases, the gdb process would hang during a fuzzing run, which can result in resource exhaustion. The gdb process is now properly killed when its timeout expires.
- BFF 1.0 discarded crashes caused by the SIGABRT signal. The reason for this was to ignore, by default, crashes that were the result of a failed assertion. However, this feature was also discarding heap corruption crashes that were caught by glibc. BFF 1.1 now investigates SIGABRT crashes to determine if they are the result of a failed assertion. Only failed assertion crashes are

discarded by default.
- The `zzuf.pl` script has been refactored for improved performance, sanity, and modularity. (Thanks Allen!)
- The BFF now performs automatic crashing testcase minimization via fuzzdiff. (Thanks Dan!)

Download BFF 1.1 [http://www.cert.org/download/bff]

About the Author

Will Dormann

✉ Contact Will Dormann [https://www.sei.cmu.edu/contact.cfm]
Visit the SEI Digital Library for other publications by Will [https://resources.sei.cmu.edu/library/author.cfm?authorID=2547]
View other blog posts by Will Dormann [/author/will-dormann]

The Software Engineering Institute (SEI) is a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD). It is operated by Carnegie Mellon University.