CERT/CC Blog

Vulnerability Insights

Updates to CERT Fuzzing Tools (BFF 2.6 & FOE 2.0.1)

POSTED ON OCTOBER 25, 2012 BY ALLEN HOUSEHOLDER [/AUTHOR/ALLEN-HOUSEHOLDER] IN TOOLS [HTTPS://INSIGHTS.SEI.CMU.EDU/CERT/TOOLS/]

Hi everybody. Allen Householder from the CERT Vulnerability Analysis [http://www.cert.org/vuls/] team here, back with another installment of "What's new in CERT's fuzzing frameworks?" Today we're announcing the release of updates of both our fuzzing tools, the CERT Basic Fuzzing Framework (BFF) [http://www.cert.org/vuls/discovery/bff.html] version 2.6 and the CERT Failure Observation Engine (FOE) [http://www.cert.org/vuls/discovery/foe.html] version 2.0.1. The remainder of this post describes the changes in more detail.

In the past, our two fuzzing frameworks had been based on related code but developed separately. Beginning with the release of BFF 2.5 [http://www.cert.org/blogs/certcc/2012/04/cert_basic_fuzzing_framework_v.html] in April and FOE 2.0 [http://www.cert.org/blogs/certcc/2012/07/cert_failure_observation_engin_1.html] in July, we began to converge these code bases back together. Today's release marks a milestone in that we have now synchronized development so that both tools are built on the same version of the underlying libraries. But all that has happened behind the scenes. What you probably care about are the new features and fixes, so let's have a look at them.

BFF 2.6 Includes CERT Triage Tools

Version 2.6 of the CERT Basic Fuzzing Framework incorporates the CERT Triage Tools [http://www.cert.org/vuls/discovery/triage.html] version 1.04. Jonathan Foote's earlier post [http://www.cert.org/blogs/certcc/2012/04/cert_triage_tools_10.html] explains how this GNU Debugger (GDB) extension classifies Linux application bugs by severity. With the addition of the CERT Triage Tools to BFF, we

have added automatic exploitability classification to our Linux fuzzing platform. BFF's GDB output now classifies crashing test cases into one of four categories: Exploitable, Probably Exploitable, Probably Not Exploitable, and Unknown.

BFF 2.6 Improves Virtual Machine Reboot Recovery

BFF 2.6 also incorporates improvements to fuzzing campaign recovery following a virtual machine reboot. In the past, the rangefinder and seedfile data was not consistently retained, and this led to a BFF campaign to recover its machine-learned data following each reboot. That is no longer the case. Learned parameter selection data is cached and recovered following a reboot so the campaign can pick up where it left off. You can read more about the underlying machine learning algorithm in our recently published SEI technical note *Probability-Based Parameter Selection for Black-Box Fuzz Testing* [http://www.sei.cmu.edu/library/abstracts/reports/12tn019.cfm].

BFF 2.6 and FOE 2.0.1 Support Configurable Timeouts for Minimization

Because minimization is a heuristic-based solution, some minimization runs can take a long time to complete. Time spent minimizing is time spent not fuzzing, and we'd rather be fuzzing than squeezing out a few more bytes from a test case. Benefitting from the integrated code base mentioned above, BFF 2.6 and FOE 2.0.1 include a new configuration option that allows the system to monitor and terminate a minimization if a timeout is exceeded. The default timeout is one hour, which should be long enough to minimize all but the most stubborn cases.

FOE 2.0.1 Improves drillresults.py

FOE 2.0 introduced the `drillresults.py` script to pick out crashes that are most likely to be exploitable and list those cases in a ranked order. FOE 2.0.1 fixes a bug in `drillresults.py` that could have caused it to overlook some interesting cases.

To use this script, run
```
tools\drillresults.py
```

For command-line usage, run
```
tools\drillresults.py --help
```

Both Platforms Reflect Bug Fixes

Spoiler alert: Software has bugs. Even software that finds bugs has bugs. BFF and FOE are no exception to this. We have fixed the ones we found since their respective prior releases. Most of these were minor, but one notable fix was that crash recycling wasn't working as well as we had intended in BFF 2.5 and FOE 2.0. We've fixed that in BFF 2.6 and FOE 2.0.1.

Read the Quick Start Instructions

Quick start instructions for both tools can be found on their download pages: BFF 2.6

[http://www.cert.org/download/bff/], FOE 2.0.1 [http://www.cert.org/download/foe/].

Contact Us

If you have any questions or comments, please feel free to contact us [mailto:cert@cert.org?subject=CERT%2FCC%20BFF%202.6%20Feedback%20INFO%23817809].

About the Author

Allen Householder

Contact Allen Householder [https://www.sei.cmu.edu/contact.cfm]
Visit the SEI Digital Library for other publications by Allen [https://resources.sei.cmu.edu/library/author.cfm?authorID=4483]
View other blog posts by Allen Householder [/author/allen-householder]