

CERT FOE - Failure Observation Engine

The CERT Failure Observation Engine (FOE) is a software testing tool that finds defects in applications that run on the Windows platform. FOE performs mutational fuzzing on software that consumes file input. (Mutational fuzzing is the act of taking well-formed input data and corrupting it in various ways looking for cases that cause crashes.) The FOE automatically collects test cases that cause software to crash in unique ways, as well as debugging information associated with the crashes. The goal of FOE is to minimize the effort required for software vendors and security researchers to efficiently discover and analyze security vulnerabilities found via fuzzing.

At the CERT/CC, we have used the FOE infrastructure to find a number of critical vulnerabilities in products such as Adobe Reader, Flash Player, and Shockwave player; Microsoft Office and Windows; Google Chrome; Oracle Outside In; Autonomy Keyview IDOL; Apple QuickTime; and many others. See [Public Vulnerabilities Discovered Using FOE](#).

Source Code

Source code for BFF and FOE can be found at at <https://github.com/CERTCC/certifuzz>.

Issues can be reported at <https://github.com/CERTCC/certifuzz/issues>.

More information about FOE

- [FOE 2.1 Release Notes](#) — CE RT Failure Observation Engine (FOE) Significant changes
- [FOE 2.1 Windows Readme](#)
- [FOE Blog posts](#)
- [Public Vulnerabilities Discovered Using FOE](#)

Download FOE

This software package contains both the source code for the distribution and a binary installer package for Windows. The installer package will attempt to install FOE and its dependent software packages on the system.

If you wish to evaluate the binary installer, it is highly advisable to do so on a non-enterprise system devoted solely to testing.

An ISO image is also available for convenient use within a Windows virtual machine instance.

Source Code

GitHub

Other Links

- [CERT Basic Fuzzing Framework BFF - GitHub](#)
- [Failure Observation Engine \(FOE\) tutorial - YouTube](#)
- [\[PDF\] Fuzz Testing for Dummies - fuzzing.info](#)
- [Let's Fuzz: IrfanView | SingleHop](#)
- [New CERT Tools Help Developers Find Vulnerabilities | SecurityWeek.Com](#)
- [A Basic Distributed Fuzzing Framework for FOE - Adobe Blogs](#)