



UNIVERSAL FUZZER



DON'T LET ATTACKS TAKE YOU BY SURPRISE

Corrupt files are one of the oldest and most effective methods of attacking company networks. Simply clicking on a weblink with malicious picture-files or opening harmless-looking PDF files sent as email attachments is enough to trigger these attacks. Protocol attacks do not require any user interaction. Simply having coding errors or vulnerabilities in your software is enough.

The attacks vary, but they all have in common is that the initial access is always enabled by a software vulnerability. Attacks against unknown, zero-day vulnerabilities have the most damaging effects, because there are no defenses against them.

FIND AND FIX CRITICAL VULNERABILITIES PROACTIVELY

The most effective way to protect your systems against zero-day attacks is find and discover unknown, zero-day vulnerabilities in your systems proactively. Fuzzing is a technique used by hackers to find unknown vulnerabilities. Fuzzing your own software before deployment or integration will make the software more robust and secure.

The Universal Fuzzer enables both software vendors and corporations using their products to test file formats and devices and software used to read them. By doing this software vendors can improve the quality of their products compared to their competitors and companies can avoid attacks that could compromise their reputation and sales.

[Learn more »](#)

CODENOMICON Ltd.
info@codenomicon.com
www.codenomicon.com

Tutkijantie 4E
FIN-90590 OULU
FINLAND
+358 424 7431

12930 Saratoga Avenue, Suite B-1
Saratoga, CA 95070
UNITED STATES
+1 408 252 4000

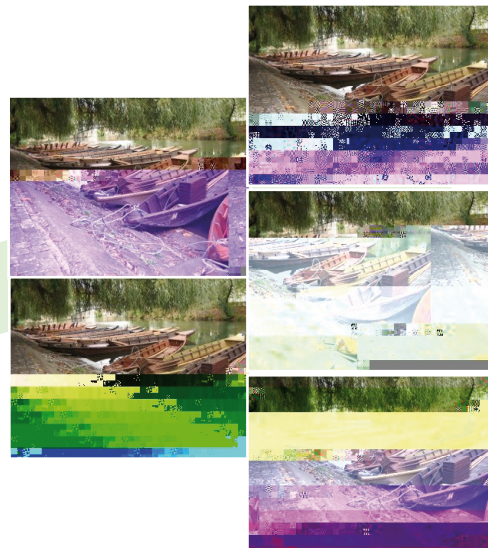
25/F., Queen's Road Centre
152 Queen's Road Central
HONG KONG
+852 3426 22900

Key Features

- » **TESTS ANYTHING:** If you can present the data in file format, then you can test it with the universal fuzzer. Use the Universal Fuzzer to test image files, captured protocol messages, text documents, wireless frames, etc.
- » **INTELLIGENT FUZZING:** Most fuzzers only perform random mutation fuzzing. The Codenomicon Universal Fuzzer utilizes heuristics to determine data structures, thus it is able to generate more intelligent test cases.
- » **EASY TO CREATE AND EXECUTE:** The Universal Fuzzer does not require any protocol specific customization. Test cases are automatically generated from sample template files.
- » **BROAD COVERAGE:** The Universal Fuzzer utilizes 15 different Fuzzers to generate test cases giving you a broad spread of what types of attacks your software will have to endure.
- » **CLEAR GUI AND AUTOMATED REPORTING FEATURES:** The Universal Fuzzer can be run through the Defensics GUI making it easy to control 15 fuzzers simultaneously. You will also the benefit of Defensics' automated reporting features: simply click on a link in the report to reproduce test vulnerabilities.
- » **DIFFERENT TEST EXECUTION METHODS:** The test cases can be run directly at the test target, or they can be injected using network connection. The test cases can also be sent using our built-in HTTP server.

Testing with the Universal Fuzzer

- » **Select your sample files. The more sample files you have, the more accurate the tests.**
- » **Choose how many test cases you want to run**
- » **Decide which fuzzers you want to use and which ratio**
- » **Generate test cases and choose how you want to execute them**
- » **Report and mitigate**



Benefits

FOR SOFTWARE DEVELOPERS

- » **DISCOVER REAL THREATS:** The main strength of Fuzzing is its unparalleled ability to find unknown vulnerabilities. Thus, you can find vulnerabilities at the earliest possible moment giving you more time to create and implement patches.
- » **HARDEN SYSTEMS BEFORE COMMERCIAL DEPLOYMENT:** The costs of bad Quality of Service (QoS) and downtime can be considerable to your company reputation and sales. Discover flaws and create patches for them proactively, before problems occur and flaws can be exploited.

CORPORATIONS

- » **IMPROVING QOS:** The costs of bad Quality of Service (QoS) and downtime can be considerable to your company reputation and sales. With Codenomicon DEFENSICS™ you can identify and fix vulnerabilities proactively, before any problems occur.
- » **AVOIDING DOWNTIME:** By finding and mitigating security issues proactively, you can anticipate upcoming patch releases. No longer making patch deployment a constant crisis management process.
- » **COMPARING VENDORS:** It is advisable to perform fuzzing on devices and software, before integrating them into your network, to see how robust and secure they are. Fuzzing can also be used for vendor selection.