

DEFENSICS 3.0

Take Your Security Testing to a New Level

Since 2001, Codonomicon DEFENSICS™ test platform has been applying fuzzing techniques to provide preemptive security testing for network equipment manufacturers, operators, consumer electronics companies, enterprises and governmental organizations.

Codonomicon's heritage lies in university research, in the OUSPG/PROTOS research project started in 1996. During the last 12 years, both in academia and in a commercial environment, our world-class group of researchers has brought to life multiple ground-breaking advances in the field of software security and quality assurance. The original PROTOS research was pioneering work which raised awareness about software vulnerabilities both in technical and governmental communities. PROTOS represents the first systematic method for finding vulnerabilities in bulk.

True to the pioneering spirit of our academic research background, Codonomicon has been defining the way for preemptive security testing ever since, being the first company to roll out commercial standard tools for such areas as wireless protocol and digital media format testing. Today, DEFENSICS remains unparalleled both in breadth of protocol coverage and efficiency of finding new flaws, covering more than 140 interfaces and remaining the winner in head-to-head bakeoffs against other fuzzing technologies.

In the world of fuzzing, even the best can do better. Codonomicon DEFENSICS 3.0 bundles our accumulated experience from the past decade and takes security testing to a completely new level. The single most important aspect of fuzzers and security testing tools is their ability to find software vulnerabilities before the tested product hits the market. Improving test coverage and efficiency even further than before has been a key goal in the development of DEFENSICS 3.0. During the process, even our own researchers have been amazed by the amount of new flaws DEFENSICS 3.0 is finding from test targets which have previously been thought well-hardened.

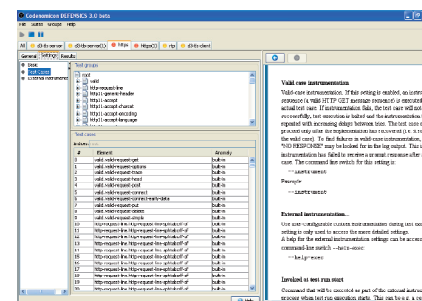
In addition to improved efficiency, DEFENSICS 3.0 introduces several major enhancements in the areas of productivity, usability, and root cause analysis. DEFENSICS 3.0 is also easier to integrate with customer testing frameworks and test control systems. With the all-new DEFENSICS 3.0 tests, users can both extend the testing capabilities from what is offered by default, but also enjoy from an improved out-of-the-box experience. Our Test Case Editing feature provides a targeted approach for testing highly specific protocol areas, whereas the Instrumentation Script Library feature enables additional means for monitoring and controlling the system under test and test execution itself. A complete rewrite of our GUI provides a dashboard view with full control over multiple test runs with multiple protocols and file formats. Advances in reporting as well as the adoption of industry standard scoring mechanisms such as CVSS and CWE aid in assessing the severity and root cause of any found problems.



3.0

Highlights

- Improved Test Coverage and Efficiency
- DEFENSICS Suite Monitor
- Test Case Editing
- Hunter Mode
- XML Anomalization Engine
- Known Vulnerabilities Test Suites
- New Reporting Engine
- PCAP I/O
- Instrumentation Script Library
- Vulnerability Validation
- End-to-End Test Engine
- Support for Many New Protocols and File Formats



Improved Test Coverage and Efficiency

DEFENSICS 3.0 takes a radical new approach to test cases. While our testing is still based on deep protocol models and systematic coverage of all possible elements, messages and message sequences, the user can now specify how many test cases he wants DEFENSICS 3.0 to generate. For busy users, a small but broad set of tests can be useful. For those with more testing time available, coverage can be made as efficient as possible. The amount of created test cases can also be specified for each covered specification separately, making it possible to focus on critical parts of the protocol or file format. DEFENSICS 3.0 Test Suites also broaden the overall specification coverage from the previous DEFENSICS releases, enabling optimal security assessment of any tested interfaces.

DEFENSICS Suite Monitor

The new dashboard approach in DEFENSICS 3.0 UI centralizes the control of multiple test suites and test reports under a single unified user interface. Multiple test suites can be configured and executed simultaneously, and all configurations can be stored for later use in test plans. Results from all test runs are archived and can be easily revisited and compared with other test runs using the DEFENSICS Suite Monitor.

Test Case Editing

Modifying existing test cases and adding completely new, custom cases has been an often-wished extension to previous DEFENSICS versions. With DEFENSICS 3.0 we are making test case editing as easy as possible for our customers. While our pre-built test cases with new, improved coverage have been created to be more than sufficient for most users, sometimes there may be a need to test certain custom protocol structures or add new test cases. With DEFENSICS 3.0, this is now possible.

Hunter Mode

Software may fail when it encounters a specific test case, but what exactly are the boundaries of the failure? How much shorter or longer overflows still make the software fail? These are important questions when attempting to find the root cause and the implications of any failure. DEFENSICS 3.0 helps in answering these questions by doing automated searches for the exact boundary values failures.

XML Anomalization Engine

XML is an ever more pervasive way of communication, used both in standard and custom application-to-application protocols. DEFENSICS 3.0 adds XML protocol testing capabilities for both standard protocols like XMPP and proprietary protocols used in many organizations. Our bold move to the application space adds a fourth dimension to our existing offering, filling the void between digital media and both wireless and wired network protocols.

Known Vulnerabilities Test Suites

Scanners and vulnerability feeds are the traditional methods to check if systems are patched against publicly known threats. But how to actually verify that a flaw has been fixed, that regression does not occur in a subsequent release, or that a closely related but not exactly the same system is not vulnerable? DEFENSICS 3.0 answers this question by providing active testing for known, publically reported vulnerabilities, mercilessly pinpointing the problems in similar fashion to testing for unknown threats.

New Reporting Engine

Reporting is an important feature of any test tool. DEFENSICS 3.0 continues to provide accurate information about the message sequences and data causing the problem. The new release introduces significant improvements for root cause analysis and report analysis. The severity and impact of a flaw can be analyzed with the help of industry standard CVSS and CWE scoring systems. Built-in support for comparing results and trends from multiple test runs provides an overall view on how the security and robustness of the tested system develops and evolves over time.

PCAP I/O

DEFENSICS 3.0 allows the user to capture all test traffic automatically in the industry-standard PCAP packet capture format for later analysis or reuse. Using a commonly understood format allows testers to make test data easily available for developers or even third parties, aiding in fault reproduction, upstream problem reporting and subsequent fixing of any found flaws.

Instrumentation Script Library

Over time we at Codenomicon have developed together with our customers various scripts for extending the tool capabilities and controlling test subjects and the test runs. Examples of this include items like automatic restarting of test subjects, machine-assisted log analysis, performance monitoring during a test run, automation of client-side testing, and much more. DEFENSICS 3.0 packages these developments inside an easy-to-apply script library that can be easily used as-is, or as a starting point for developing custom scripts.

Vulnerability Validation

When a testing team finds a problem from a system under test, one of the key tasks is to report the problem with enough detail for developers to reproduce it. DEFENSICS 3.0 Vulnerability Validation allows exporting of failed cases into a miniature Test Suite that can be executed by R&D to reproduce the failure. These miniature Test Suites are of course fully configurable, making them usable also in environments that are not exact replicas of the environment used by the original testing team.

End-to-End Test Engine

The testing of firewalls, proxies and even complete networks just got a whole lot easier with the groundbreaking DEFENSICS 3.0 End-to-End Test Engine. This feature allows the user to easily simulate both ends of a protocol session while monitoring the effects of test traffic on any SUTs in between. Any changes to the test traffic itself can also be monitored, enabling the user to visualize what elements in the network are able to block malicious traffic or allowing it to pass.

Support for Many New Protocols and File Formats

DEFENSICS 3.0 introduces several new protocols, expanding the DEFENSICS usage to completely new areas. Some of the examples include vCard, vCal and iCal for extending our handset testing portfolio, WiMAX for further strengthening our line of wireless protocol testers, as well as all-new XML-based SOAP and XMPP tests.

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

Tutkijantie 4E | FIN-90570 OULU | FINLAND | +358 424 7431
10670 North Tantau Avenue | Cupertino, CA 95014 | UNITED STATES | +1 408 252 4000
25/F, Queen's Road Centre | 152 Queen's Road Central | HONG KONG | +852 3426 22900