Peach Fuzzer 3.9 Updates

Datasheet

What's new in Peach Platform v3.9 (2016 Q1)

The Peach Fuzzer Q1 release includes a good mix of new features, improvements, and new Pits. The new Pits are available for licensing singularly or as part of a Pit Pack. To access new Pits that have been added to previously licensed Pit Packs, re-download Peach Fuzzer at dl.peachfuzzer.com.

Fuzzing Definitions (Pits)

Descriptions of the new Pits follow:

DICOM File

Digital Image and Communications in Medical (DICOM) is an image format based on medical industry standards. It is commonly used for medical images in a large variety of medical equipment.

DICOM Network

Digital Image and Communications in Medical (DICOM) is an image format based on medical industry standards. It is commonly used for medical images in a large variety of medical equipment.

HL7v2

Health Level Seven (HL7) is a data format commonly used in the healthcare industry to store electronic health records, billing information, and other information. Patient records and other data relevant to running a medical operation are included.

DTLS Server (SSL)

DTLS is a derivation of SSL protocol. It provides the same security services (integrity, authentication and confidentiality) as SSL/TLS but under the UDP protocol. This pit is available as part of SSL.

iSCSI

iSCSI (Internet Small Computer System Interface) works on top of the Transport Control Protocol (TCP) and allows the SCSI command to be sent end-to-end over local-area networks (LANs), wide-area networks (WANs), or the Internet.

Professional/Enterprise

Descriptions of new features and improvements for Professional and Enterprise follow:

Tuning Weights UI

A new configuration option has been added to allow tuning of the messages and fields being fuzzed. Options include increasing or decreasing the focus of testing and also excluding testing fields altogether. The feature is available from the configuration screen menu as "Tuning".

Peach Fuzzer 3.9 Updates

Datasheet

Library UI Improvements

The Library screen in the Peach application has several changes to improve usability. The Pits are now displayed in a column view and a search/filter feature has been added to allow quick access.

New Configuration Format

This quarter we are introducing a new configuration file with an extension of .peach. Going forward, the Web UI will create and save these .peach files. From the command line you have the option of directly running a Pit (.xml files) or running a .peach configuration.

Existing users will notice the Library page will list any existing configurations in a "Legacy" section. Clicking on a legacy configuration will prompt a conversion workflow to generate a new .peach file.

Fault Details UI Changes

Some minor changes have been made to the fault detail page. The field and mutation algorithms used when the fault occurred are now displayed.

Updates to minset Tool

The minset tool has been updated to use an improved minimization-set algorithm. Additionally, several bugs have been fixed that caused minset to use incorrectly calculated addresses.

New duration Command Line Switch

A new command line argument --duration has been added in this release to make CI integrations easier. The duration argument will cause Peach to run for a specific length of time and then exit. Duration is specified in days, hours, and minutes.

Address Sanitizer

Several changes to add support for Address Sanitizer (ASan) compile time instrumentation has occurred:

- SSH Command monitor now supports ASan
- ASan is now enabled by default for SSH Command, Process, and Run Command monitors.
- Support for GCC integrated ASan has been added

Peach Multi-Node CLI Tool

A new command line tool has been added that allows the control of multiple Peach instances. The tool is available in the sdk/tools/peachcli folder.

- Push configurations from a master node to slave nodes
- Group multiple nodes by name so they can be operated on together
- Start, stop and pause jobs by group or specific node
- Pull all faults into a common log folder

Jira Integration Scripts

A python based tool peach2jira has been added to export faults into Jira tickets. This is useful when integrating Peach into CI or traditional build systems. The tool is available in the sdk/tools/peach2jira folder.

Developer

The following features require a developer license and are intended for advanced users who are creating custom Peach Pits.

Interactive REST API Documentation

Interactive REST API documentation has been added to Peach using the Swagger system. The interactive REST API documentation provides forms to call the APIs and also show any available documentation. The documentation is available from a running Peach instance at /swagger. Example: http://127.0.0.1:8888/swagger.

SSL Publisher ALPN Support

Support for the Application-Layer Protocol Negotiation Extension (ALPN) has been added to the SSL Publisher. ALPN is needed to fuzz protocols such as HTTP v2. ALPN is exposed as a parameter, see the SSL Publisher documentation for additional information.

Rest Publisher Extensions

The REST publisher has been updated to support Web APIs that require XML instead of JSON content types. Additionally, the content type can now be customized, allowing support for non-standard payloads, binary data, etc.

New JSON Elements

New JSON elements have been added in an effort to improve JSON support in Peach. These elements are now recommended over the older Json element.
The following new data elements are available for modeling JSON documents:

- JsonObject
- JsonArray
- JsonString
- JsonInteger
- JsonDouble
- JsonBool