Peach Fuzzer 4.0 Updates

Datasheet

What's new in Peach Platform v4.0 (2016 Q2)

This is our second release of 2016. It 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. If you are interested in using a new Pit that has been added to an existing Pit Pack already licensed, re-download Peach Fuzzer by visiting https://dl.peachfuzzer.com.

Fuzzing Definitions (Pits)

Descriptions of the new/updated Pits follow:

HL7 v2 XML

Expanding on our Health Level Seven (HL7) support, this new pit fuzzes XML representations of health records. Pipehat-formatted records are already supported by an existing pit.

HL7 Network

HL7 records are commonly transported via Minimal Lower Layer Protocol (MLLP) and TCP. This new pit fuzzes both Content Receivers and Content Senders.

ZIP and CAB

We've added new pits for the ZIP and CAB archival file formats. As with the other file-fuzzing pits, they both start from a configurable set of sample files and generate test cases by parsing and mutating them.

DICOM Updates

C-STORE fragmentation support has been added to support sending large DICOM files to targeted Service Class Providers. Improved field names to clarify presentation in the UI and reports.

SSL/TLS Expanded Cipher Support

The cipher suites supported by the SSL/TLS pits have been expanded in this release. The following table shows the current list of supported ciphers:

ID	Cipher Suite	Prot	Key Ex	Au	Enc	Mac
0xC0,0xAC	ECDHE_ECDSA_WITH_AES_128_CCM	TLSv1.2	ECDH	ECDSA	AESCCM(128)	AEAD
0xC0,0xAE	ECDHE_ECDSA_WITH_AES_128_CCM_8	TLSv1.2	ECDH	ECDSA	AESCCM(128)	AEAD
0xC0,0xAD	ECDHE_ECDSA_WITH_AES_256_CCM	TLSv1.2	ECDH	ECDSA	AESCCM(128)	AEAD
0xC0,0xAF	ECDHE_ECDSA_WITH_AES_256_CCM_8	TLSv1.2	ECDH	ECDSA	AESCCM(128)	AEAD

ID	Cipher Suite	Prot	Key Ex	Au	Enc	Mac
0xC0,0x23	ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2	ECDH	ECDSA	AES(128)	SHA256
0xC0,0x09	ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLSv1.0	ECDH	ECDSA	AES(128)	SHA1
0xC0,0x27	ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	ECDH	RSA	AES(128)	SHA256
0xC0,0x13	ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.0	ECDH	RSA	AES(128)	SHA1
0x00,0x9C	AES128-GCM-SHA256	TLSv1.2	RSA	RSA	AESGCM(128)	AEAD
0x00,0x3C	AES128-SHA256	TLSv1.2	RSA	RSA	AES(128)	SHA256
0x00,0x3D	AES256-SHA256	TLSv1.2	RSA	RSA	AES(256)	SHA256
0x00,0x2F	AES128-SHA	TLSv1.0	RSA	RSA	AES(128)	SHA1
0x00,0x35	AES256-SHA	TLSv1.0	RSA	RSA	AES(256)	SHA1

Professional/Enterprise

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

New Major Version

This release marks a new major version number for Peach. It includes a number of breaking changes and deprecated elements/features. Make sure to check out the Breaking Changes section of this datasheet.

Edit/Copy/Delete Pit Configuration

It is now possible to edit, copy, or delete an existing Pit configuration from the Library page in the Peach Web Interface. Hover over a Pit configuration to find the new icons that enable this functionality.

PitTool

PitTool is provided as an additional set of utilities useful for developing Peach pits.

analyzer: Run a Peach analyzer.

compile: Validate and compile pit into .meta.json and .ninja files.

crack: Crack a sample file.

makexsd: Generate a peach.xsd file.

ninja: Create a sample ninja database.

Fragmented Protocol Support

This release introduces a new element and two new action types allowing fragmented protocols to be easily modeled and fuzzed. The *Frag* element, *outfrag* action type, and *infrag* action type have been added.

APC Power Monitor

The *APC Power* monitor switches outlets on an APC power distribution unit (PDU) on and off via SNMPv1. This monitor is useful for automatically power cycling devices during a fuzzing session. APC's Switched Rack Power Distribution Unit (AC7900) is known to work with this monitor.

SNMP Power Monitor

The SNMP Power monitor switches outlets on a power distribution unit (PDU) on and off via SNMPv1. This monitor is useful for automatically power cycling devices during a fuzzing session.

Web Fuzzing/RESTful Fuzzing Improvements

In this release we continue to add features related to web fuzzing and specifically RESTful service fuzzing. Changes include new analyzers to speed up creation of fuzzing definitions and also changes to the related publishers to enable fault detection on return status codes.

Renamed Rest Publisher to WebApi Publisher

The Rest publisher has been renamed to WebApi publisher. The old name is an alias and will continue to work.

Improvements to HTTP and WebApi Publishers

Both the HTTP and WebApi publishers have been updated this release cycle to include:

- Fault on HTTP status code. Status codes can be configured.
- Fail on HTTP status code. Status codes can be configured.
- Expose Headers collection for easy modification from Python scripts.

Swagger Analyzer

This analyzer converts Swagger API JSON into Peach Pits for fuzzing WebApi style web service endpoints. Swagger is a popular method for representing your RESTful API, especially for documentation purposes. Many frameworks can export Swagger API representations which can then be converted into partial pits using this analyzer.

Postman Analyzer

This analyzer converts Postman Collections into Peach Pits for fuzzing WebApi style web service endpoints. Postman is a popular app used during development and testing of WebApi style web services. APIs are organized into Collections which can be converted into fuzzers using this analyzer.

GDB Server Monitor
Specific support for the GDB Server protocol.

GDB Script Exposed
Both GDB monitors now support changing the script used to drive GDB during fuzzing.

Breaking Changes
This release introduces a number of breaking changes and deprecated features. This section contains a list of the major changes that have occurred.

Peach Agent
The Peach Agent server process has been moved into a separate executable (PeachAgent.exe). The old method of running peach -a tcp is deprecated.

Deprecated Command Line Switches
The following command line switches are deprecated:

-t
The test switch has been removed.

-c
The count switch has been removed. The default and recommended strategy do not have this concept.

-p
Parallel switches have been removed. These are not needed with the default strategy.

Plugins Folder
The location for plugins has changed in this release. In the past, plugins were discovered and loaded from the same folder as the Peach assemblies. Now, plugins are loaded from a separate Plugins folder under the Peach installation folder.

Sample Ninja
The Sample Ninja database creation tool (named PeachSampleNinja.exe in the past) has been merged into the new PitTool.exe.