Release Notes for Cisco Security Packet Analyzer 6.3(2)

Revised: January 18, 2018

This document supports the release of the Cisco Security Packet Analyzer 6.3(2) image. This is a full image that can be used for initial or recovery installation, as well as for upgrading an existing installation from the Security Packet Analyzer 6.2(2), 6.2(3), or 6.3(1) releases.

Version 6.3(2) includes new features and bug fixes, and introduces support for the Virtual Security Packet Analyzer.

Contents

1 Cisco Security Packet Analyzer 6.3(2) Image Contents

The Cisco Security Packet Analyzer 6.3(2) image contains the following changes over 6.3(1):

- New Features and Functionality
  - Introduced Virtual Security Packet Analyzer, a VM appliance version of Security Packet Analyzer with support for VMware ESXi and KVM hypervisors.
  - Added the ability to create a packet query directly on a host or conversation-related bar chart. The query uses the host IP(s) from the bar chart and the duration in the dashboard's Interactive Filter.
  - Added the ability to replay a pcap file onto the network. For example, this can be used to replay captured packets to a firewall or IDS for further testing or analysis.

- Updated Features and Functionality
  - Improved packet query performance by implementing search indexes on monitored hosts.
  - Improved usability of the file reconstruction pop-up window, which now offers more user guidance.

- General Bug Fixes
  - Fixed a system crash issue caused by fragmented IP packets.
  - Fixed a core dump issue when running "show configuration" after "config clear".
  - Fixed an issue with scheduled export jobs disappearing after a system reboot.
  - Fixed an error when saving filtered packets in the capture decode window.
  - Fixed issues with capturing to files on external iSCSI storage.
  - Fixed a test connectivity failure when submitting managed device info.
  - Fixed a SPAN creation issue when there are multiple managed-devices.
  - Fixed a "no interface data" error for managed devices with SNMPv3 AuthNoPriv or SNMPv3 NoAuthNoPriv.
  - Fixed an issue with custom web server port configuration not being carried across an image upgrade.

- Security Bug Fixes
  - CSCvh20057 – Linux Kernel Loaded ELF Executables Local Privilege Escalation Vulnerability (CVE-2017-1000253)
  - CSCvh00264 – Multiple Vulnerabilities in Samba (CVE-2017-14746, CVE-2017-15275)
  - CSCvh00332 – PHP timelib_meridian Function Heap Buffer Overflow Vulnerability (CVE-2017-16642)

- Browser Compatibility
  - Firefox ESR 45 and 52
  - Internet Explorer 11
  - Chrome 62 and 63 (unofficial support)
    - SECPA software is tested against Chrome during development. However, Chrome cannot be officially supported because it has no long-term stable release series – Chrome users are generally automatically upgraded to the latest release, which may contain breaking changes that cannot be anticipated.

2 Upgrading Cisco Security Packet Analyzer from 6.2(3) or 6.3(1) to 6.3(2)

To upgrade a Cisco Security Packet Analyzer from the 6.2(3) or 6.3(1) releases to the 6.3(2) release, place the 6.3(2) software upgrade (.bin.gz) image on an FTP, HTTP, or SCP/SFTP server and issue the CLI command

upgrade <*image-url*>

Both configuration data and packet capture data will be carried over from the old release to 6.3(2) when upgrading this way. This is recommended for most users.

If you prefer a fresh install of the application image (i.e., existing configuration and packet capture data will **not** be carried over), issue the CLI command

upgrade <*image-url*> reformat

With the **reformat** option, **both configuration data and packet capture data will be lost. Ensure that your configuration data is backed up and packet capture data is downloaded and saved as needed.**

Note: After upgrading from 6.2(3) to 6.3(2), the telnet service will be disabled by default to meet Cisco product security requirements. Use the CLI command “exsession on” to re-enable the telnet service if needed.

3 Upgrading Cisco Security Packet Analyzer 6.2(2) to 6.3(2)

To upgrade a Cisco Security Packet Analyzer from the 6.2(2) release to the 6.3(2) release, place the 6.3(2) image on an FTP, HTTP, or SCP/SFTP server and issue the CLI command

upgrade <*image-url*> reformat

Ensure that the "reformat" option is passed. This option is required when upgrading from 6.2(2) to 6.3(2) in order to support capture performance improvements. However, it will result in the loss of all existing capture data. **Before upgrading to 6.3(2), ensure that your configuration data is backed up and packet capture data is downloaded and saved as needed.**

4 Verifying Cisco Security Packet Analyzer 6.3(2) Installation

To verify that the Cisco Security Packet Analyzer 6.3(2) image was installed successfully, log in to the CLI console and execute the "***show version***" command. The following version details should appear:

SECPA application image version: **6.3(2)** RELEASE SOFTWARE **[fc9]**

5 Known Issues in Release 6.3(2)

CSCvh17008	scheduled exports sometimes sent based on UTC instead of local system timezone
CSCvh32860	PTP time sync not working on SECPA 2420 and 2440 appliances
CSCvh59626	GUI upgrade doesn't work

6 Obtaining Documentation, Support and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.