Release Notes for Cisco Security Packet Analyzer 6.3(1)

September 27, 2017

This document supports the release of Cisco Security Packet Analyzer 6.3(1) version. This can be used for initial installation, as well as for upgrading an existing installation of Cisco Security Packet Analyzer 6.2(2) or 6.2(3) release.

This version of 6.3(1) includes new features, bug fixes and performance improvements.

Cisco Security Packet Analyzer 6.3(1) release

The Cisco Security Packet Analyzer 6.3(1) release contains the following changes over 6.2(2) and 6.2(3):

- New Features and Functionality:
  - Added the ability to perform application upgrades and apply patches via the GUI, without an external server to host the release or patch file. Note that upgrades from 6.2(2) or 6.2(3) to 6.3(1) requires a server to host the release file.
  - Added Japanese UI localization.
  - The capture sessions page is now the home page.
  - When creating a new capture session, the parameters needed for one maximum-size continuous capture-to-disk session are populated by default.
  - Added packet capture rate to GUI and API.
  - Added logging of capture query activity to the audit trail, available via GUI and API.

  - Added a separate **Capture Query** user permission.
  - Added Stealthwatch terminology (i.e., Subject/Peer as well as Source/Destination) in capture query dialog for clarity.
  - Added packet capture runtime statistics, such as actual storage used by a capture session.
  - Added the ability to reconstruct a file transferred via FTP, HTTP, or SMB. The file to be reconstructed is selected from a list of detected file transfers on the **Capture** > **Packet Capture** > **Decode** > **Files Reconstruction** screen.
  - Added the ability to decrypt a packet capture file containing SSL/TLS traffic. Only RSA-encrypted traffic is supported, and the corresponding RSA private key must be provided. After decryption, the file reconstruction function can be applied if desired. This feature is accessed via the **Decrypt** button on the **Capture** > **Packet Capture** > **Decode** > **Files** screen.
  - Added the ability to upload an external pcap file for analysis on the SECPA. This is performed with the **Upload** button on the **Capture** > **Packet Capture** > **Decode** > **Sessions or Capture** > **Packet Capture** > **Decode** > **Files** screens.
  - Added application transaction analysis for DNS, DHCP, RADIUS, 802.1x, ARP, ICMP, HTTP, FTP, SMB, LDAP, and Kerberos.
  - Added HTTP, FTP, and SMB file transfer transaction analysis.
  - Added analysis of TLS and other secure protocol negotiations.
  - Added support for IPv6 ERSPAN.
  - Added support for scheduled reports on detailed views.
  - Added a configuration option to exclude encapsulations, such as VLAN and MPLS labels, from flow identification.
  - Added the ability to invert the sense of a software capture filter (i.e., exclude matching packets).
  - Added an SNMP test button/message for adding multiple managed devices.
  - Added a UI popup indicator while system processes are restarting.
- Updated Features and Functionality:
  - Refreshed GUI look and feel.
  - Updated NBAR2 application classification engine and signatures.
  - Improved vNAM data port ERSPAN stability and performance.
  - Rebuilt the capture partition RAID formats. The RAID rebuild no longer requires a subsequent reformat or recovery install of the application.
- Removed Features and Functionality:
  - Removed WAAS support.
  - Removed SMB1 file sharing support due to security issues.
- Packet Capture Performance Improvement:

  This release brings the sustained and lossless packet capture rate to 14Gbps.
- General Bug Fixes:
  - Fixed an issue with decoding NetFlow packets requiring templates.
  - Some fixes for voice/video monitoring and additions to video call and media stream correlations.
  - Fixed IPv6 ERSPAN parser.

  - Fixed ESXi multiple queues issue.
  - Fixed sliced packets issue.
  - Fixed an issue with capture sessions disappearing after reboot.
  - Fixed an issue with the debug port agent overwriting the aggregation configuration.
  - Fixed an issue with managed devices which was not functional.
  - Fixed an issue with the NIC clock not syncing to the Linux clock.
  - Fixed an issue with a non functional **shutdown** CLI command.
  - Fixed an intermittent issue with a non functional **tracerout** CLI command.
  - Fixed an issue with the REST API **nbi-system** endpoint not redirecting to the correct product name.
- Security Bug Fixes:
  - Fixed the path traversal issue (ZDI-CAN-4918).
  - Fixed the Samba RCE issue (CVE-2017-7494).
- Browser Compatibility:
  - Firefox ESR 45 and 52
  - Internet Explorer 11
  - Chrome 60 and 61

Note SECPA is not supported with Chrome, as Chrome recommends its user to periodically upgrade to the latest release and does not support long-term stable release series.

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

Note The upgrade procedure depends on whether you are upgrading from 6.2(2) or 6.2(3). Use the **show version** CLI command to verify the current software version.

To upgrade a Cisco Security Packet Analyzer from the 6.2(3) release to the 6.3(1) release, It is recommended to place the 6.3(1) image on an FTP/HTTP/SCP/SFTP server and run the CLI command as follows:

upgrade <image-url>

Both configuration data and packet capture data will be carried over from 6.2(3) to 6.3(1).

If you prefer to reinstall the application (i.e., existing configuration and packet capture data will not be carried over), run the CLI command as follows:

upgrade <image-url> reformat

Note 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.

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

To upgrade a Cisco Security Packet Analyzer from the 6.2(2) release to the 6.3(1) release, it is recommended to place the 6.3(1) image on an FTP/HTTP/SCP/SFTP server and run the CLI command as follows:

upgrade <image-url> reformat

Ensure you passed the **reformat** option. This option is required when upgrading from 6.2(2) to 6.3(1) in order to support capture performance improvements. However, it will result in the loss of all existing capture data.

Note Before upgrading to 6.3(1), ensure that your configuration data is backed up and packet capture data is downloaded and saved.

Verifying Cisco Security Packet Analyzer 6.3(1) Installation

To verify if Cisco Security Packet Analyzer 6.3(1) 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(1) RELEASE SOFTWARE [fc6]

Obtaining Documentation, Support and Security Guidelines

For information on accessing documentation, contacting support team, providing documentation feedback, security guidelines, and accessing 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.