SECURE ENDPOINT RELEASE NOTES

Version 5.4

25 May 2022

Secure Endpoint Windows Connector 7.5.5

New

- Added support for Windows 10 IoT Enterprise. See Secure Endpoint Windows Connector OS Compatibility for additional information.

  IMPORTANT! The connector on IoT Enterprise does not support HORM, UWF, Orbital, and the Kenna Risk Score. See Incompatible Software and Configurations.

- Beginning in Windows Connector 7.5.5, end users will no longer be able to read the contents of the policy.xml file. Policy information can only be accessed by users with privileges to view and edit the policy in the Secure Endpoint Console. Exclusions will still be visible in the connector IP Tray user interface unless this setting is disabled in policy settings (Hide exclusions can be found under Client User Interface).

  IMPORTANT! If you require the policy.xml file to remain readable by all users in your organization, contact support.

- This version of the Secure Endpoint Windows connector is the last to support legacy operating systems such as Windows 7 and 8, Server 2012, and all 32-bit versions of Windows.

25 May 2022

Bugfixes/Enhancements

- Increased stack size for some processing threads to prevent crashing while scanning some in-memory archives. (CSCwb43257)
- Japanese language wording fixed in user interface. (CSCwb33742)
- Cache enhancements.
- Performance improvements to process cache.
- Updated AMPCLI tool responses to include more information from the connector engines.
- Fixed policy sync to properly use auto-detected proxies as specified by the system. (CSCwa97557)
- Addressed an issue with malicious Ethos file detections not being quarantined if seen more than once.
- Adjusted a filter regex to prevent a catastrophic backtrace exception from stopping client powershell scripts.
- Updated support diagnostic tool so that it does not require elevated privileges.
- Fixed an issue where remote file fetch is not working if the file being fetched is not quarantined.
- Fixed exploit prevention engine compatibility issues with McAfee.
- Improved exploit prevention engine for:
  - Script control functionality (wmi detection in plugins/macros).
  - Atom bombing protection mechanism.
  - User access control bypass mechanism (false positive reduction).
  - Performance enhancements.
  - Handling a potential crash in Windows 7.
- Reduce memory usage on computers that have larger amounts of available memory, such as servers.
- Update ClamAV to 0.103.5, including fixes for the following security vulnerabilities:
  - CHM Infinite Loop (CVE-2022-20770). CSCwa48226
  - Crash when scanned file is truncated (CVE-2022-20796). CSCwa22202
  - TIFF infinite loop (CVE-2022-20771). CSCwa70702
  - HTML/javascript parser leak (CVE-2022-20785). CSCwa70706

11 May 2022

Secure Endpoint Console 5.4.20220511

New

- Added new application exclusion type to exclude specified applications from exploit prevention protection.

  IMPORTANT! Organizations that had application exclusions created for them by support will now have a custom exclusion set named Exploit Prevention Custom applied to all policies with exploit prevention enabled.

- Released API version 3.

Bugfixes/Enhancements

- Fixed an issue with validation for Mac and Linux wildcard exclusions.
- Improved the date range behavior in a policy's product update when changing product versions.
- Fixed a defect where the policy serial number was not incremented when exclusions were modified.
- Minor cosmetic and alignment fixes.
- Fixed an issue where the time slider was not displaying properly for mobile app trajectory.

5 May 2022

Secure Endpoint iOS Connector 1.6.0

Bugfixes/Enhancements

- Updated Umbrella to 1.6.0. See the Umbrella release notes for details: https://support.umbrella.com/hc/en-us/articles/5743040028948

27 April 2022

Secure Endpoint Console 5.4.20220427

Bugfixes/Enhancements

- Redesigned the policy list page with improved responsiveness. Users can now see the names of IP lists applied to a policy even if they don't have permission to edit the list.
- Fixed an issue where some unsupported Windows versions were displaying erroneous Kenna Risk Score and associated vulnerability information. Currently, only Windows 10 is supported for vulnerability inference based on Build and Update Build Revision information.

26 April 2022

Secure Endpoint Linux Connector 1.19.0

New

- Added official support for Debian 10 and 11.
- Added official support for openSUSE Leap 15.
- Added official support for SUSE Linux Enterprise 15.

See Cisco Secure Endpoint Linux Connector OS Compatibility for supported operating systems and kernel versions for this release.

Bugfixes/Enhancements

- Removed rename event monitoring within containers on RHEL/CentOS/OL 6 to ensure a more consistent view of filesystem activity from the host namespace. (CSCwa36470)

19 April 2022

Secure Endpoint Android Connector 2.4.0

Bugfixes/Enhancements

- The connector can now upload problem reports that were requested remotely.
- Enhanced support for Android 12.
- Minor bugfixes and performance improvements.

13 April 2022

Secure Endpoint Console 5.4.20220413

Bugfixes/Enhancements

- Improved console global search for applications.
- Minor bugfixes and performance improvements.

12 April 2022

Secure Endpoint Mac Connector 1.18.1

Bugfixes/Enhancements

- Fixed an issue where ClamAV definition updates may fail if the computer has a large /etc/passwd file. (CSCwb13792)
- Fixed an issue where the events history in the Agent UI does not show the events that happened on the selected from date.
- Updated CiscoSSL to 1.1.1n.7.2.390, including changes related to the vulnerability described in CVE-2022-0778.

Secure Endpoint Linux Connector 1.18.1

Bugfixes/Enhancements

- Updated CiscoSSL to 1.1.1n.7.2.390, including changes related to the vulnerability described in CVE-2022-0778.

30 March 2022

Secure Endpoint Console 5.4.20220330

Bugfixes/Enhancements

- Improved navigation and usability for users who belong to multiple Secure Endpoint organizations. This includes the ability to set a default organization to speed up the login process.
- Added operating system version to the computers API.
- Minor Device Trajectory bug fixes and improvements.
- Minor dark mode, alignment and font issue fixes.

16 March 2022

Secure Endpoint Console 5.4.20220316

New

- Added support for wildcard process exclusions for Secure Endpoint Windows Connector 7.5.3 and later.

Bugfixes/Enhancements

- Fixed global search results for Mobile App Trajectory.
- Minor dark mode and alignment issue fixes.
- Improved accessibility of the user menu and feedback widget.

Secure Endpoint Windows Connector 7.5.3

New

- New capability to send additional Microsoft Windows update build revision information to improve risk-based OS vulnerability interference capability.
- Behavioral Protection engine updated to be able to detect command line argument spoofing.
- The connector now supports wildcards (‘*’) in Process Exclusions. This wildcard will not expand beyond path separators.

Bugfixes/Enhancements

- Updated the exploit prevention engine.
- Exclusion performance enhancements.
- Fixed a bug that caused Outlook to crash when exploit prevention was enabled.

- Addressed an issue where clients were experiencing a blue screen on Windows Server 2012 with the exploit prevention driver when upgrading to 7.5.1. (CSCwa59221)
- Addressed an issue that caused exploit prevention to fail to after a connector upgrade. (CSCvz83877)
- Fixed an issue where the connector was causing unexpected reboots on Windows Server 2016. (CSCwa86504)
- Improved the uninstall process of the connector.
- Added support for the BypassIO feature in Windows 11.
- Fixed a crash in the connector when performing an IOC scan.
- Fixed a bug that would cause the connector to crash if it was updating a policy during shutdown.
- Fixed a bug in the self-protect driver during shutdown crashes of the connector.
- Corrected Japanese wording in the IP Tray. (CSCwa86562)

Secure Endpoint Mac Connector 1.16.3

Bugfixes/Enhancements

- Updated ClamAV to 0.103.5, including changes related to the vulnerability described in CVE-2022-20796.

Secure Endpoint Linux Connector 1.17.2

Bugfixes/Enhancements

- Fixed an issue where ClamAV definition updates may fail if the computer has a large /etc/passwd file. (CSCwb13792)
- Updated ClamAV to 0.103.5, including changes related to the vulnerability described in CVE-2022-20796.

3 March 2022

Secure Endpoint Mac Connector 1.18.0

New

- The connector has been rebranded to Cisco Secure Endpoint. This includes some functional changes like the Application directory name for the Mac connector. See Cisco Secure Endpoint Mac Connector Rebrand for details.

Bugfixes/Enhancements

- Fixed an issue where the connector would continue to send detection events for a network connection after the remote IP was removed from the block list.
- The Support Tool will no longer leave temporary work files on the computer when run.
- Reduced volume and frequency of disk writes when accessing internal connector database files.
- Fixed an issue where process exclusions could incorrectly apply matches to child processes.

Secure Endpoint Linux Connector 1.18.0

New

- Added support for Oracle Unbreakable Enterprise Kernels (UEK) on Oracle Linux 7 and 8.
- Added official support for AlmaLinux 8.3 and higher.
- Added official support for Rocky Linux 8.4 and higher.

See Cisco Secure Endpoint Linux Connector OS Compatibility for supported operating systems and kernel versions for this release.

Bugfixes/Enhancements

- Added support for CPU Accounting-enabled computers. (CSCwa91004)
- Removed rename event monitoring within containers on RHEL/CentOS/OL 7 to ensure a more consistent view of file system activity from the host name space. (CSCwa36470)
- Extended support for sysadmins to build the connector's file system and network kernel modules for unsupported UEKs. See Building Cisco Secure Endpoint Linux Connector Kernel Modules for more information.
- Reduced volume and frequency of disk writes when accessing internal connector database files.
- Fixed an issue where the Orbital service would fail to start after a successful installation due to a missing configuration file.
- Eliminated erroneous error log messages when the connector is freshly installed and Orbital is enabled.

- Fixed an issue in the network flow monitor where the connector could fail to monitor parents of forked processes that existed before the ampdaemon starts.
- Fixed a memory leak that occurred when registering connectors on Amazon Linux 2.
- Fixed an issue where process exclusions could incorrectly apply matches to child processes.

2 March 2022

Secure Endpoint Console 5.4.20220302

New

- Added one-click integration with SecureX to allow your Secure Endpoint data to be shared and viewed in the SecureX console.
- Incident promotion allows high and critical incidents to be promoted to SecureX threat response incident manager to be streamlined and enriched.

Bugfixes/Enhancements

- Minor bugfixes and performance improvements.

16 February 2022

Secure Endpoint Console 5.4.20220216

Bugfixes/Enhancements

- Added Windows Server 2022 to the operating system filters on the computers page.
- Minor bugfixes and performance enhancements.

2 February 2022

Secure Endpoint Console 5.4.20220202

Bugfixes/Enhancements

- Added Windows 11 to the operating system filters on the computers page.

25 January 2022

Secure Endpoint Linux Connector 1.17.1

New

- Added support for Ubuntu 18.04 LTS using kernel versions 4.18 and higher. See Cisco Secure Endpoint Linux Connector OS Compatibility for supported operating systems and kernel versions for this release.

19 January 2022

Secure Endpoint Console 5.4.20220119

Bugfixes/Enhancements

- Changed Significant Compromise Artifacts to Significant Compromise Observables for added clarity.
- Accessibility and visual improvements to device trajectory status indicators and icons.
- Rebranded Threat Grid to Secure Malware Analytics.

Archived release notes

Previous years release notes can be found at the following links:

- 2021 release notes
- 2020 release notes
- 2019 release notes
- 2018 release notes
- 2017 release notes
- 2016 release notes
- 2015 release notes
- 2014 release notes
- 2013 release notes