AMP for Endpoints Release Notes

2020

15 December 2020

AMP for Endpoints Mac Connector 1.14.1

Bugfixes/Enhancements

- New alert icon for the menulet user interface.
- Use legacy kernel extensions on all versions of macOS 10.15. This fixes third-party software compatibility issues seen when the new system extensions API is used on macOS 10.15.
- Fixed an issue that could result in high CPU/memory usage when the Connector is unable to connect to the AMP Network Extension on macOS 11.0.
- Improve fault guidance when unable to connect to the AMP Network Extension on macOS 11.0.
- Connectors on macOS 11.0 now report the operating system version correctly.
- Fixed an issue that could cause Time Machine to backup to a remote drive or Time Capsule to fail.
- When running the uninstaller from a service, users will now be prompted twice to remove the AMP System Extensions, allowing the Connector to uninstall cleanly.

AMP for Endpoints Linux Connector 1.15.0

New

- Added beta support for Ubuntu 20.04.0 LTS and 20.04.1 LTS.

IMPORTANT! The Ubuntu support in this release is intended for evaluation in non-production environments only. Feedback from this beta will be included in a new release with full Ubuntu support in January 2021. To provide feedback, contact support. See this article for more information.

Bugfixes/Enhancements

- Fixed a crash related to the use of process exclusions.
- Fixed an issue where Advanced Custom Detection updates were not processed until Connector restart.

8 December 2020

AMP for Endpoints Console 5.4.20201208

Bugfixes/Enhancements

- Fixed a bug that prevented users from adding customers to an MSSP business.
- Simplified Device Trajectory filters so that selecting none of the flags is now the same as selecting all of them.
- Fixed a cosmetic issue where the Device Trajectory filter button was hidden on wide screen monitors.
- The default setting for Script Control in new Windows policies is now Audit mode.

24 November 2020

AMP for Endpoints Console 5.4.20201124

Bugfixes/Enhancements

- Fixed an issue where the Quarantine Failed error reason wasn't displayed in Quarantine Failed Events. (CSCvw45177)
- Exported System Process Protection events now show the parent process path.
- Fixed an issue where Low Prevalence Detections were not rolling over to Threat Detected as expected. (CSCvw49000)
- The context menu allows you to create new outbreak control lists in place through a dialog.

- Fixed alignment in device trajectory time lines.
- Improved device trajectory scaling for higher resolution monitors.

18 November 2020

AMP for Endpoints Windows Connector 7.3.9 (supersedes 7.3.3 and 7.3.5)

Bugfixes/Enhancements

- Improved cloud registration process to prevent deadlock under high system activity. (CSCvw34067)

10 November 2020

AMP for Endpoints Console 5.3.20201110

Bugfixes/Enhancements

- Renamed Business Settings to Organization Settings.
- Fixed a bug when searching for existing APKs in Android Custom Detections.
- MSSP partners can now sort organizations by compromise percentage.

5 November 2020

AMP for Endpoints Mac Connector 1.14.0

New

- Added official support for macOS 11 (Big Sur). This release supports macOS 10.14, 10.15, and macOS 11. Mac Connector versions prior to 1.14.0 are not compatible with macOS 11.

IMPORTANT! New full disk access approvals are required after upgrading to this release on all versions of macOS. Install and grant all required permissions to the 1.14.0 Mac Connector before upgrading macOS to ensure continued protection of the endpoint.

- The Mac Connector requires new approvals for full disk access. MDM profiles must be updated to ensure continued protection. If MDM profiles are not being used the Connector will be unable to provide full protection until access has been granted by the end user. See this TechNote for details on these changes.
- This TechNote has been updated with descriptions of new Mac Connector faults.

Bugfixes/Enhancements

- Updated ClamAV to 0.102.4, including changes related to the following vulnerabilities:
  - CVE-2020-3327
  - CVE-2020-3481

29 October 2020

AMP for Endpoints Windows Connector 7.3.5 (superseded by 7.3.9)

New

- Added support for the Windows 10 October 2020 update.

Bugfixes/Enhancements

- Addressed an issue where the Connector would have trouble shutting down in a timely manner.
- Added more monitoring to Behavioral Protection to detect malicious activity:
  - Open mutex and event objects.
  - Processes listening on TCP and UDP ports.
- Behavioral Protection can now take additional actions upon detection:
  - End a target process and all its descendants.
  - Initiate a Forensic Snapshot.
- Added a feature that allows Behavioral Protection to enable Windows auditing to trace endpoint events for malicious activity. This must be activated in policies under Advanced Settings -> Engines.
- Script Control can now be set to audit, block, or disabled independently from your Exploit Prevention settings. This can be changed in policies under Advanced Settings -> Engines. (CSCvv87628)
- Connector no longer holds on to connections longer than necessary, avoiding network resource exhaustion on Windows. (CSCvv85169)
- Connector now downloads a smaller installer when deploying or updating Orbital.

27 October 2020

AMP for Endpoints Console 5.4.20201027

Bugfixes/Enhancements

- MSSP partners can access status metrics via a new API endpoint.
- MSSP provisioning API enhanced to enable MSSP partners to create new customers.
- Fixed an issue where the computer scan dialog would not close after a scan was started.
- Fixed an issue where the Diagnose button wasn't working when you navigate to a computer from the Groups page.
- Deprecated TLS 1.0/1.1 from AMP for Endpoints Console in favor of TLS 1.2 and newer.
- System Process Protection events now display the path for parent files when available.

13 October 2020

AMP for Endpoints Console 5.4.20201013

Bugfixes/Enhancements

- Behavioral Protection tooltips display relevant signature descriptions.
- Fixed SecureX ribbon issue that prevented users from interacting with pivot menu on audit logs.

1 October 2020

AMP for Endpoints Windows Connector 7.3.3 (superseded by 7.3.9)

Bugfixes/Enhancements

- Addressed a local privilege escalation vulnerability. (CSCvv53346, CVE-2021-1280)
- Addressed a rare condition where Behavioral Protection would detect a file as deleted when it wasn't actually deleted.
- The Connector no longer fills logs with error messages before Behavioral Protection signatures are downloaded.
- The Connector now sends separate notifications for script control detections with the Exploit Prevention engine.

- Fixed a bug where the Connector is disconnected for the length of the heartbeat interval after configuration changes.
- The Connector now attempts to reconnect with the Cisco cloud faster after a failure instead of waiting for the next heartbeat interval

29 September 2020

AMP for Endpoints Console 5.4.20200929

Bugfixes/Enhancements

- Minor UI improvements to the users page.
- The Get Endpoints and Find Observables buttons on the SecureX ribbon retrieve endpoints as expected.
- Product name is displayed correctly in the vulnerable software report (in console and exported CSV files).
- Fixed an issue where SHA-256 info was missing from quarantine failed events. (CSCvv77863)
- The time spans corresponding to behavioral protection events are highlighted in Device Trajectory.
- [Premier tier only] Added a welcome page to introduce users to SecureX Threat Hunting.

22 September 2020

AMP for Endpoints Linux Connector 1.13.2

Bugfixes/Enhancements

- Reduced installer size to further mitigate an issue where 1.12.0-1.12.5 Connectors may fail to upgrade via policy on slow networks. (CSCvv07225)
- Fixed issue with upload timeouts for remote file fetch and snapshot uploads over slow networks. (CSCvv17811)
- Fixed a kernel panic that can occur when unloading the ampnetworkflow kernel module on CentOS/RHEL 6/7. (CSCvv58039)
- Fixed a bug where the required kernel modules might not load on older CentOS/RHEL distributions, depending on the host kernel version. (CSCvv49913)
- Fixed a problem that would cause the Connector to consume significant amounts of memory on CentOS/RHEL 8.1 and 8.2.
- Updated ClamAV to 0.102.4, including changes related to the following vulnerabilities:
  - CVE-2020-3327
  - CVE-2020-3481

17 September 2020

Cisco Security Connector 1.5.0

Bugfixes/Enhancements

- Updated Umbrella to 1.5.0. See Umbrella release notes for details: https://support.umbrella.com/hc/en-us/sections/206928207-Release-Notes-for-Umbrella-Software

IMPORTANT! This release of the Cisco Security Connector is available for devices running iOS 13.2 and higher.

15 September 2020

AMP for Endpoints Console 5.4.20200915

New

- You can save and recall filters on the Computers page.

Bugfixes/Enhancements

- Added Behavioral Protection Demo Data.
- More details added to Behavioral Protection events.
- [Premier tier only] Exported CSV files for SecureX Threat Hunting events include a field for update/delete reason.
- SecureX ribbon updated to 1.3.0.
- Improved filter view on the Computers page.
- It is easier to make selections in the Device Trajectory interface.
- Fixes to dark mode in Device Trajectory.
- Added button to expand or collapse all rows on the Indicators page.
- Events arriving at the same time appear in the correct order on the Events page.

10 September 2020

AMP for Endpoints Android Connector 2.0.2

New

- New Activity Log for viewing events in the app.

Bugfixes/Enhancements

- The app now runs as a foreground service in the notification area.
- Reduced battery consumption in idle state.
- Improved logging for troubleshooting,
- More robust recovery from network errors.
- Added SHA-256 for detection events in AMP console.

9 September 2020

AMP for Endpoints Windows Connector 7.3.1

New

- New Behavioral Protection engine available (64-bit versions of Windows).
- Specialized Behavioral Protection events include observables, observed activity, and action taken.
- Added Behavioral Protection process exclusion type.
- Exploit Prevention engine with Audit mode support.
- Exploit Prevention engine with Script Control support.

Bugfixes/Enhancements

- Increased the number of process exclusions honored by the Connector to 500.
- Improved stability of local UI notifications.
- Addressed an issue where System Process Protection exclusions would not work for processes that start before the Connector. (CSCvt63211)
- Changed Connector driver altitudes to officially registered altitudes.
- Removed Connector-related events and logs from a computer when the Connector is uninstalled
- Addressed issues with file exclusions.
- Addressed an issue with low prevalence uploads of portable executable files (CSCvv52410)
- General performance and stability improvements for Exploit Prevention engine.
- Fix for the vulnerability described in CVE-2019-0708.

- Fixed Exploit Prevention engine compatibility issues with the following applications:
  - APTA Connect
  - MS PowerPoint 2016/2013
  - FSLogix
  - Internet Explorer and different plugins
  - CIG
  - ACG
  - MS Office Appv applications
  - Visual Studio debugger
  - Vizient and Open Text IRM
  - Black Knight
- Product upgrades no longer fail under a rare condition when the Network Flow Monitoring (NFM) driver was left behind from an old Connector that required reboots on upgrades. (CSCvv20713)

IMPORTANT! A reboot will be required for this upgrade on any computers where the Connector meets this condition.

1 September 2020

AMP for Endpoints Console 5.4.20200901

Bugfixes/Enhancements

- [Premier tier only] Computers can now be removed from a SecureX Threat Hunting Incident Report.
- [Premier tier only] The Dashboard, Inbox and Overview pages now only reflect computers in the current version of the SecureX Threat Hunting Incident Report. Events are now generated for added and deleted computers.
- Fixed layout issues on the Computers page when the filter panel is collapsed.
- Fixed alignment issues on the Dashboard and Inbox when items are muted.
- Fixed a discrepancy between the Vulnerable Software page and the CSV export. The CSV export only showed one of the observed groups even if there was more than one group.

18 August 2020

AMP for Endpoints Mac Connector 1.12.7 (supersedes 1.12.0–1.12.4)

Bugfixes/Enhancements

- Reduce installer size to further mitigate issue where 1.12.0–1.12.4 Connectors may fail to upgrade via policy on slow networks. (CSCvv37020)
- Fixed issue with upload timeouts for remote file fetch and snapshot upload over slow networks. (CSCvv17808)
- Patched ClamAV 0.102.3 to include changes related to the following vulnerabilities:
  - CVE-2020-3481
  - CVE-2020-3327

AMP for Endpoints Console 5.4.20200818

Bugfixes/Enhancements

- [Premier tier only] Threat Hunting incidents table updated with headers.
- [Premier tier only] Users subscribed to Critical Announcements receive an email when a Threat Hunting incident is updated.
- [Premier tier only] Deleted computers are removed from the Threat Hunting incident report and the timeline. The computers and timeline sections of the Threat Hunting incident report are hidden if there are no computers remaining.
- [Premier tier only] Fixed IE 11 compatibility issues with Threat Hunting timeline.
- [Premier tier only] Added a full description to supplementary Orbital links in Threat Hunting.
- Fixed Computer Management page rendering issue when there is only a single computer.
- SecureX ribbon updated to 1.2.3.
- The “Need Connector Update” metric on the Computer Management page counts unsupported Connectors.

IMPORTANT! The number of Connectors that need updates are higher than before because unsupported Connectors are now counted.

11 August 2020

AMP for Endpoints Linux Connector 1.12.7 (Supersedes 1.12.0-1.12.5)

Bugfixes/Enhancements

- Reduce installer size to further mitigate issue where 1.12.0-1.12.5 Connectors may fail to upgrade via policy on slow networks. (CSCvv07225)
- Fixed issue with upload timeouts for remote file fetch and snapshot upload over slow networks. (CSCvv17808)
- Patched ClamAV 0.102.3 to include changes related to the following vulnerabilities:
  - CVE-2020-3481
  - CVE-2020-3327

6 August 2020

AMP for Endpoints Windows Connector 7.2.13

Bugfixes/Enhancements

- Fixed a privilege escalation vulnerability. (CVE-2020-3350, CSCvt98752)
- Improved TETRA definition update mechanism by dropping buggy ciphers from the update servers. (CSCvu75358)
- Made stability and efficacy improvements to the Malicious Activity Protection engine.
- Resolved Exploit Prevention engine compatibility issues with the following applications:
  - Powershell System.Management.Automation.Runspaces.LocalRunspace
  - PDF API and HTML to PDF Converter for .NET (EO.Pdf.dll)
- Updated Exploit Prevention engine to address the vulnerability described in CVE-2020-14418. (CSCvu61848)

4 August 2020

AMP for Endpoints Console 5.4.20200804

Bugfixes/Enhancements

- [Premier tier only] The SecureX Threat Hunting Incident Report was reformatted for a better user experience. The date the analyst discovered the incident and the date the incident started have also been clarified.
- Fixed a time stamp discrepancy between events in the console and the downloaded CSV files.
- Event export CSV files were renamed when the export consists of a single file.
- Reduced the footprint of the SecureX ribbon to reduce overlap with other elements of the Console.
- Policy Save/Cancel buttons have been repositioned to improve the integration with the SecureX ribbon.

21 July 2020

AMP for Endpoints Console 5.4.20200721

New

- [Premier tier only] Users receive an email notification for new Threat Hunting incidents if they are subscribed to Critical Issues in their announcement preferences.
- [Premier tier only] Users can navigate from each event in the timeline section of Threat Hunting reports to the corresponding time stamp in Device Trajectory if the event is within the last 30 days.
- Added a policy setting to enable a button in the Windows Connector UI to update TETRA definitions on demand. Only available for Windows Connector 7.2.11 and higher.
- IP List Create and Update Audit Logs show the specific IP addresses that were added and deleted from the list.

> **IMPORTANT!** The first 1000 added IP addresses and 1000 deleted IP addresses are displayed per audit log before the list is truncated.

Bugfixes/Enhancements

- Device Trajectory Event Listing displays proper labels for system events.
- Fixed alignment issues with statistics on Dashboard and with Policy Product Updates.
- Dates in Device Trajectory do not scroll out of view.
- Threat Detected in Low Prevalence has been added to Device Trajectory.

21 July 2020

AMP for Endpoints Linux Connector 1.13.1

Bugfixes/Enhancements

- Fixed realtime filesystem and network monitoring when running the Connector on RHEL 7.9 beta releases.
- Fixed a timeout issue that could cause failures when upgrading the Connector via policy on slow networks (CSCvv07225).
- The installer removes stale database files when upgrading from an older version of the Connector (CSCvu98581).
- The Connector now scans all local storage devices and logical volumes during a full scan.
- Reduced Connector CPU and disk space usage when the associated user of a process exclusion does not exist on the system.
- Updated ClamAV to 0.102.3, including changes related to the vulnerability described in CVE-2020-3341.

AMP for Endpoints Linux Connector 1.12.6

Bugfixes/Enhancements

- Fixed realtime filesystem and network monitoring when running the Connector on RHEL 7.9 beta releases.
- Fixed a timeout issue that could cause failures when upgrading the Connector via policy on slow networks (CSCvv07225).
- The installer removes stale database files when upgrading from an older version of the Connector (CSCvu98581).
- The Connector now scans all local storage devices and logical volumes during a full scan.
- Reduced Connector CPU and disk space usage when the associated user of a process exclusion does not exist on the system.
- Updated ClamAV to 0.102.3, including changes related to the vulnerability described in CVE-2020-3341.

AMP for Endpoints Mac Connector 1.12.6

Bugfixes/Enhancements

- Fixed a timeout issue that could cause failures when upgrading the Connector via policy on slow networks (CSCvv07225).
- The installer removes stale database files when upgrading from an older version of the Connector (CSCvu98581).
- The Connector now scans all local storage devices and logical volumes during a full scan.

- Reduced Connector CPU and disk space usage when the associated user of a process exclusion does not exist on the system.
- Updated ClamAV to 0.102.3, including changes related to the vulnerability described in CVE-2020-3341.

7 July 2020

AMP for Endpoints Console 5.4.20200707

New

- [Premier tier only] The Threat Hunting timeline view displays user information. When the user data is not available, the view displays a label “Unknown”.
- [Premier tier only] Threat Hunting events appear in the dashboard, inbox, and overview pages as a new event type for each hunt.

  IMPORTANT! Threat Hunting events cannot be muted like other event types.

- [Premier tier only] The Threat Hunting incidents report obeys the user time zone settings. Users can click the time display on console pages to access time-related functionality.
- Failure Events in exported Events CSV have error codes.

Bugfixes/Updates

- Fixed discrepancies between license information displayed on the license page vs. displayed on the weekly/monthly/quarterly reports.
- To make the presentation of events more consistent between the Events tab, CSV export and the API, all events are displayed as separate independent events. (Before this version, a detection event followed by a quarantine event was displayed as a single event. As of this version, these events are displayed separately.)
- Audit logs for **automated actions - triggered forensic snapshot** display the user correctly.

25 June 2020

AMP for Endpoints Windows Connector 7.2.11 (supersedes 7.2.5 and 7.2.7)

New

- Added support for Windows 10 May 2020 Update (Version 2004)

Bugfixes/Updates

- For policy upgrades the Connector honors the time zone on the endpoint rather than assuming UTC-0. (CSCvt59185)
- File properties are filled out for AMP Connector DLLs.
- Addressed crash that could sometimes occur when Connector is configured to use a proxy to communicate with the AMP Cloud.
- Addressed issue where Connector upgrades could hang indefinitely.
- Addressed issue where an identity sync error could cause the Connector to hang on shutdown.
- Addressed issue where some DLL files were not removed after uninstalling the Windows Connector.
- Connector generates driver logs on agent start up if configured to in the policy.
- Cleaned up signal handling in Proxy Discovery.
- Performance improvements for Script Protection.
- Addressed issue where System Process Protection exclusions would not work for processes that start before the AMP Connector. (CSCvt63211)
- Update driver altitude to fix compatibility issue against other AV. (CSCvt99262)
- Fixed Connector crash caused by long network interface names. (CSCvu15646)
- Fix to prevent ClamAV log files from filling up disk space. (CSCvu65043)
- Updated Exploit Prevention Engine to include changes related to the vulnerability described in CVE-2020-0796.
- Resolved Exploit Prevention engine compatibility issue with:
    - ExOpen
    - Outlook VBA plugin

IMPORTANT! A recent change to log handling caused disk space to fill up during high scan activity. This has been fixed in v7.2.11. (CSCvu65043)

Cisco recommends upgrading all v7.2.5 & v7.2.7 Connectors to v7.2.11 to avoid issues related to disk space.

---

24 June 2020

AMP for Endpoints Console 5.4.20200624

Bugfixes/Updates

- Fixed issue where MSSP partners were not able to see more than 25 customers on the MSSP partner page. (CSCvu61075)
- Updated list of processes protected by and excluded from the AMP for Endpoints Windows Exploit Prevention engine.

  New Protected Processes:

  - Microsoft HTML Application Host
  - Windows Script Host
  - Microsoft Assembly Registration Tool
  - Zoom
  - Skype
  - Slack
  - Cisco Webex Teams
  - Microsoft Teams

  The engine also monitors the following directories:

  - Windows AppData Temp Directory (\Users\[username]\AppData\Local\Temp\)
  - Windows AppData Roaming Directory (\Users\[username]\AppData\Roaming\)

  The following processes are excluded from Exploit Prevention monitoring because of compatibility issues:

  - McAfee DLP Service
  - McAfee Endpoint Security Utility

  IMPORTANT! This change will be included when you change the Exploit Prevention conviction mode to block, or the next time you save a policy that already has Exploit Prevention set to block. Until then the existing list will be used.

9 June 2020

AMP for Endpoints Console 5.4.20200609

New

- When exporting events to a CSV file, you will now receive an email containing a link to download an archive file containing one or more CSV files depending on the number of events.

Bugfixes/Updates

- Fixed an issue that prevented users from disabling file fetch from the Business Settings page. (CSCvu21445)
- Fixed an erroneous warning about moving iOS devices to a new group when no iOS devices were being moved. (CSCvu01056)
- Improved performance when loading the Computers page summary for an organization with a large number of Connectors installed.

27 May 2020

AMP for Endpoints Console 5.4.20200527

Bugfixes/Enhancements

- CSV exports for Events will now be handled via a download link emailed to the user.
- Some list pages now use a floating pagination bar to allow increased visibility.

AMP for Endpoints Linux Connector 1.13.0

New

- Added official support for RHEL/CentOS/Oracle Linux 8.1 and 8.2. The kernel-devel package must be installed on these systems to enable realtime network and file monitoring. A Connector fault will be raised if this package cannot be found. See Linux Kernel-Devel Fault for more information.
- Automatic crash reporting is available when the Connector is running on RHEL/CentOS/Oracle Linux 7 and 8. The setting is enabled by default and can be found in Administrative Features under Advanced Settings in Linux Connector policies.

20 May 2020

AMP for Endpoints Linux Connector 1.12.5 (superseded by 1.12.7)

New

- Added official support for RHEL/CentOS/Oracle (RHCK) Linux 7.8. See AMP for Endpoints Linux Connector OS Compatibility and AMP for Endpoints Compatibility with RHEL/CentOS/Oracle Linux 7.8 for more information.

12 May 2020

AMP for Endpoints Console 5.4.20200512

Bugfixes/Enhancements

- The Conviction Mode for Script Protection in new policies now defaults to Quarantine.
- Orbital install events are now reported correctly for unsupported operating systems.
- Clicking a file name in Device Trajectory will highlight the row.
- Minor UI fixes for dark mode.

11 May 2020

AMP for Endpoints Mac Connector 1.12.4 (superseded by 1.12.7)

Bugfixes/Enhancements

- Fixed a memory leak that could occur when setting up a proxy.

AMP for Endpoints Linux Connector 1.12.4 (superseded by 1.12.7)

Bugfixes/Enhancements

- Fixed an issue in the redirfs kernel module affecting Connector version 1.12.3 on RHEL/CentOS 6 that could cause the computer to hang with high CPU utilization. You must reboot the computer after upgrading for the changes to take effect. (CSCvu07130)
- Fixed a memory leak that could occur when setting up a proxy.

28 April 2020

AMP for Endpoints Console 5.4.20200428

New

- Added a policy setting to allow the Malicious Activity Protection engine to monitor network drives.

IMPORTANT! This setting will be enabled when you change the MAP conviction mode to audit, block, or quarantine or the next time you save a policy that already has MAP set to audit, block, or quarantine. Until then, it will not be enabled.

Bugfixes/Enhancements

- Automated Actions logs now store 30 days of events.
- Fixed an issue that sometimes prevented child groups from being selected in Automated Actions.
- Updated the list of processes protected by the AMP for Endpoints Windows Connector Exploit Prevention engine.

> **IMPORTANT!** This change will be included when you change the Exploit Prevention conviction mode to block, or the next time you save a policy that already has Exploit Prevention set to block. Until then the existing list will be used.

16 April 2020

AMP for Endpoints Windows Connector 7.2.7 (superseded by 7.2.11)

New

- Added support for Windows 10 20H1 Update (Version 2004) (Preview build: 19041.173).

Bugfixes/Enhancements

- Malicious Activity Protection (MAP) engine performance improvements.
- Resolved an issue where the Connector service would freeze on startup under certain circumstances. (CSCvt38340)
- Fixed an installer issue that failed to send reboot completed and update completed events when a reboot is required on upgrade.
- Windows Connector now reports the correct processor ID of the computer.

AMP for Endpoints Android Connector 2.0.1

New

- Added Export Logs in left navigation menu to help with diagnosis of any Connector issues.

Bugfixes/Enhancements

- Fix for a provisioning error that could occur on upgrades using an APK without an embedded policy.
- Fixed an error that could cause a Scan Failed message when the device is left on overnight.

14 April 2020

AMP for Endpoints Console 5.4.20200414

New

- Added Automated Action to move compromised computers to a different group.

7 April 2020

AMP for Endpoints Windows Connector 7.2.5 (superseded by 7.2.11)

Bugfixes/Enhancements

- Fixed an issue where the Connector could cause a fatal system error when used in conjunction with software that use file system locks as part of their normal operation. (CSCvt56075)
- Improved uninstall logic to gracefully handle Orbital uninstall failures that could block the Connector uninstall.

IMPORTANT! The nature of the error in 7.2.3 requires a reboot of the computer when upgrading to 7.2.5 or any later version. Note that you can use the Reboot Delay setting in policy to defer when computers reboot but you cannot use the Block Update if Reboot Required setting. If you experience fatal stop errors when uninstalling or upgrading you can uninstall in Safe Mode or contact support for help.

AMP for Endpoints Mac Connector 1.12.3 (superseded by 1.12.7)

Bugfixes/Enhancements

- Fixed a connection failure due to invalid activation code after new install (CSCvt29571).
- Added ID numbers to fault information displayed in the ampcli.

AMP for Endpoints Linux Connector 1.12.3 (superseded by 1.12.7)

New

- Added official support for Oracle Linux 6.10 Red Hat Compatible Kernel (RHCK). Oracle UEK is not supported.

Bugfixes/Enhancements

- Fixed a rare kernel panic on RHEL/CentOS 6 when the Connector service is frequently restarted (CSCvt54122).
- Fixed a connection failure due to invalid activation code after new install (CSCvt29571).
- Added ID numbers to fault information displayed in the ampcli.

3 April 2020

AMP for Endpoints Console 5.4.20200403

Bugfixes/Enhancements

- Added a theme control to user account settings to switch to dark mode manually.

31 March 2020

AMP for Endpoints Console 5.4.20200331

New

- Added Automated Action to send files involved in a compromise to Threat Grid for analysis.
- Dark mode is available on browsers that support it on Windows, macOS, and iOS versions that include it.

Bugfixes/Enhancements

- Fixed an issue that caused the CSV file export from the Vulnerable Software page to be empty. (CSCvt30917)
- Added support for deploying the Cisco Security Connector through Microsoft Intune.
- Added more time options to the Reboot Delay under Product Updates in Windows policies.

27 March 2020

Cisco Security Connector 1.4.4

Bugfixes/Enhancements

- Updated Umbrella https://support.umbrella.com/hc/en-us/articles/360049108311-Cisco-Security-Connector-for-iOS-Version-1-4-4 (no changes to Clarity.)

IMPORTANT! This release of the Cisco Security Connector is available for devices running iOS 13.2 and higher.

19 March 2020

Cisco Security Connector 1.4.3

Bugfixes/Enhancements

- Cisco Security Connector
  - Localization of UI to Korean, Traditional Chinese, Japanese, Russian, Italian, German, French, Spanish and Portuguese.
  - Dark mode support.
- Clarity
  - Improved secure communication between the Connector and AMP Cloud.
  - Network monitoring now includes flow direction (available with iOS 13).

IMPORTANT! This release of the Cisco Security Connector is available for devices running iOS 13.2 and higher.

17 March 2020

AMP for Endpoints Console 5.4.20200317

New

- Automated Action to isolate compromised endpoints.
- Added ability to stop endpoint isolation in bulk.

Bugfixes/Enhancements

- Added support for AMP for Endpoints Android Connector 2.0 to Device Trajectory.
- Added more events for AMP for Endpoints Android Connector 2.0.
- Added policy settings to allow script protection to be turned off or run in audit mode.

AMP for Endpoints Android Connector 2.0.0

New

- Full native integration with the AMP Cloud.
- New UI design.
- Support for Android version 6.0 and above, including the latest Android 10.
- Supports activation of Google Play Store version of Connector for all regions.
- One-click configuration when downloaded from Google Play.
- Increased performance when scanning apps.
- Improved secure communication between the Connector and AMP Cloud.
- Supports SHA-256 fingerprint scanning.

IMPORTANT! AMP for Endpoints Android Connector 2.0 does not support upgrading from v1.x. You must uninstall previous versions before installing 2.0.

AMP for Endpoints Windows Connector 7.2.3 (superseded by 7.2.5)

New

- Improved secure communication between the Connector and AMP Cloud.

Bugfixes/Enhancements

- Updated Connectivity Test Tool with new command line arguments and output.
- Script protection across the local endpoint, attached storage, and network.
- Fixed an issue where ClamAV was taking long time in scanning PDF files resulting into longer high CPU usage. (CSCvs33228)
- Addressed issue where Windows Connector would fail to upgrade when installed alongside BitDefender AV. (CSCvs58858)
- Fixed an issue with ClamAV where scanning a certain zip file was crashing Windows connector. (CSCvs34538)
- Resolved an issue where having %temp% path set to different drive than primary drive will fail the Windows Connector upgrade. (CSCvs62397)
- Updated ClamAV to 0.102.1, including changes related to the vulnerability described in CVE-2019-15961.

- Resolved Exploit Prevention engine compatibility issues with the following applications:
  - CyberArk
  - Forcepoint Insider Threat
  - Diva Client
  - AppV
  - Outlook VBA Plugin
  - Universal Windows Platform apps
  - Articad
  - Macros In Excel 365
  - BIFIT signer plugin in Microsoft Internet Explorer

3 March 2020

AMP for Endpoints Console 5.4.20200303

Bugfixes/Enhancements

- Fixed a problem with some Mac and Linux Connector 1.12 installer packages that would leave new Connector installs unable to connect to the AMP Cloud. This issue only affects new Connector installs on an endpoint and does not affect Connector upgrades. Affected customers will receive a separate announcement that references CSCvt29571.
- Added more information to Automated Actions action log entries and a link to the event in Device Trajectory.
- CSV downloads from the Events page now include indicator tactics and techniques.
- Improved the operating system name entry in the computer panel to be more accurate. (CSCvo56525 & CSCvr29801)

26 February 2020

AMP for Endpoints Mac Connector 1.12.2 (superseded by 1.12.7)

Bugfixes/Enhancements

- Fixed an issue where deleting a file on a locally-hosted network share was incorrectly identified as an execute event.
- Fixed an issue where scripts were incorrectly identified as Mach-O files in execute events.
- Fixed an issue with process exclusion monitoring that could result in an ampdaemon restart in certain scenarios.

AMP for Endpoints Linux Connector 1.12.2 (superseded by 1.12.7)

New

- Added official support for Oracle Linux 7.7 Red Hat Compatible Kernel (RHCK). Oracle UEK is not supported.

Bugfixes/Enhancements

- Fixed an issue where some rename operations would not trigger an on-access scan.
- Fixed a CentOS/RHEL 6 kernel panic from the redirfs kernel module that can occur when drives are frequently mounted and unmounted.
- Fixed a CentOS/RHEL 7 kernel panic from the ampfsm kernel module that can occur when unloading the kernel module while performing a rename operation (CSCvt13313).
- Fixed an issue with process exclusion monitoring that could result in an ampdaemon restart in certain scenarios.

18 February 2020

AMP for Endpoints Console 5.4.20200218

New

- The Automated Actions page lets you set actions that trigger when compromise events at a specified severity level occur on Windows endpoints in selected groups. The initial release includes the ability to automatically generate Forensic Snapshots when a Windows endpoint with Orbital enabled is compromised. (Advantage package only)

Bugfixes/Enhancements

- Orbital Advanced Search and Forensic Snapshots are now available in the AMP for Endpoints Windows Connector in APJC. (Advantage package only)

  IMPORTANT! Existing AMP for Endpoints customers can enroll to access Orbital Advanced Search and Forensic Snapshot for the remainder of their license period at no charge. Refer to this FAQ for further information.

- The Indicators page has been updated with links to the Dashboard, Events, and Inbox tabs filtered to computers that observed the specific Cloud Indications of Compromise.
- Global search results now include Cloud Indications of Compromise, tactics, and techniques.

- Cloud Indications of Compromise descriptions, including tactics and techniques, have been added to Device Trajectory, Dashboard, Inbox, and Events listings.
- Selecting an event in Device Trajectory highlights the entire activity line so you can more easily see which system the event relates to.
- The AMP for Endpoints Console UI has been updated to use a new look and feel.
- Connector filenames have been updated to take the format amp_groupname.extension.

4 February 2020

AMP for Endpoints Console 5.4.20200204

New

- A new Indicators page maps Cloud Indications of Compromise (IOCs) to the MITRE ATT&CK knowledge base of tactics and techniques. You can search the knowledge base by indicator name, tactics, and techniques.

23 January 2020

AMP for Endpoints Linux Connector 1.12.1 (superseded by 1.12.7)

Bugfixes/Enhancements

- Fixed a problem that could reduce the effectiveness of process exclusions in some situations.
- Fixed a situation that could add unnecessary delay in quarantining malicious files when the Cloud connection is unreliable. (CSCvs75040)
- Updated third-party libraries, including changes to libxml2 related to the following vulnerability:
  - CVE-2019-19956

AMP for Endpoints Mac Connector 1.12.1 (superseded by 1.12.7)

Bugfixes/Enhancements

- Report the Connector's unique hardware identifier as part of Connector registration.
- Fixed rare crash limited to 1.12.0 Mac Connector. (CSCvs61368)
- Fixed a situation that could add unnecessary delay in quarantining malicious files when the Cloud connection is unreliable. (CSCvs75040)

- Performance improvements for systems with many repeating execute events.
- Improved handling of corrupt AMP kernel extension files detected on the system during install/upgrade.

21 January 2020

AMP for Endpoints Console 5.4.20200121

Bugfixes/Enhancements

- Forensic snapshots now include additional information.
- Added filtering for Endpoint Isolation to the audit log.

7 January 2020

AMP for Endpoints Console 5.4.20200107

New

- AMP for Endpoints is now available as two packages – AMP for Endpoints Essentials and AMP for Endpoints Advantage. Existing customers will become AMP for Endpoints Essentials customers and retain all current features and capabilities. Refer to this FAQ for further information.
- Orbital Advanced Search is now available on Windows in NAM and EU. (Advantage package only)

IMPORTANT! Users who were enrolled in the Orbital Advanced Search beta must uninstall the beta Connector (6.5.1) and perform a clean install of AMP for Endpoints Windows Connector 7.1.5. Upgrading from the beta Connector to 7.1.5 is not supported.

- Orbital Advanced Search can be used on computers with AMP for Endpoints Windows Connector 7.1.5 and higher.
- Forensic Snapshot is now available on Windows in NAM and EU. (Advantage package only)

IMPORTANT! Existing AMP for Endpoints customers can enroll to access Orbital Advanced Search and Forensic Snapshot for the remainder of their license period at no charge. Refer to this FAQ for further information.

Release note links

Current release notes can be found here.

Other release notes can be found at the following links:

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