FIREEYE TECHNICAL DOCUMENTATION

CENTRAL MANAGEMENT

RELEASE NOTES

RELEASE 9.1

Central Management Release Notes

Software Release 9.1.0

Revision 1

FireEye Contact Information:

Website: www.fireeye.com

Technical Support: https://csportal.fireeye.com

Phone (US):

1.408.321.6300

1.877.FIREEYE

Contents

Announcements

This document provides an overview of the new features and changes in the FireEye Central Management 9.1.0 release, including any new commands, resolved issues, and known issues.

FireEye Customer Security Best Practices

Because our quality assurance process includes continuous security testing, FireEye recommends updating all FireEye products with the latest releases as soon as possible. As an overall strategy to reduce risk exposure, customers are also encouraged to follow best practices, which include:

- Always keep the product version up-to-date
- Limit network access to the management interfaces of the appliance using firewalls or similar measures
- Only issue accounts to trusted administrators
- Use strong passwords
- Monitor logs
- Restrict physical access to the appliance to trusted administrators

Models Not Supported in This Release

The following Central Management models are not supported in Release 9.1.0 and later releases.

- All CM x3xx models

Download the Security Content Bundle

After the upgrade, certain processes will be in a pending state until new security content is downloaded and installed. The security content is downloaded and installed automatically

for online customers. Offline customers must manually download and install the new security content after upgrading appliances to 9.1.0.

Upgrade

The FireEye Central Management 9.1.0 release requires a reboot for the update to take effect. You can upgrade your CM appliance to 9.1.0 from release 8.7.0 or later.

IPMI and BIOS firmware updates are required for the CM 4500 model. See the section "Upgrading IPMI 3.11 and BIOS 1.9 Firmware for Specific Platforms" below.

NOTE: After an upgrade to version 9.1.0, certain processes will be in a pending state until new security content is downloaded and installed. See "Download the Security Content Bundle" in Announcements on the previous page.

Upgrading MVX Clusters

Direct upgrade of MVX clusters (MVX Smart Grid) from an earlier release to 9.1.0 is not supported. Follow the procedure in this FireEye Community article to upgrade your MVX clusters.

Downloading Content from the DTI Offline Update Portal

If you download CM 9.1.0 security content from the DTI Offline Update Portal, use the **SCNET-2.0** channel of the portal.

CAUTION! Downloading security content from a different channel will result in a loss of detection.

For details, see the *FireEye DTI Offline Update Portal User Guide*.

Supported Appliance Versions

A CM platform running release 9.1.0 can manage the following appliance versions:

- **Network Security (NX Series):** 9.1.x, 9.0.x, 8.3.x
- **Email Security — Server Edition (EX Series):** 9.1.x, 9.0.x, 8.4.x
- **File Protect (FX Series):** 9.1.x, 9.0.x, 8.3.x
- **Malware Analysis (AX Series):** 9.1.x, 9.0.x, 8.4.x
- **Endpoint Security (HX Series):** 5.1.x, 5.0.x, 4.9.x
- **Virtual Execution:** 9.1.x, 9.0.x, 8.3.x (upgrade only)

Upgrading IPMI 3.11 and BIOS 1.9 Firmware for Specific Platforms

The CM 4500 model requires upgrades to IPMI 3.11 and BIOS 1.9. You must install the IPMI upgrade before you upgrade the BIOS. **(COM-21016, COM-25601)**

See the *Administration Guide* for the appliance for detailed instructions about upgrading IPMI.

To upgrade IPMI to version 3.11:

CAUTION! IPMI network and password settings revert to factory defaults after this upgrade, and IPMI logs are deleted. Make a note of your settings and back up your IPMI logs.

CAUTION! Do not shut down or remove power from the appliance during the upgrade.

1. Go to CLI configuration mode.

   ```
   hostname> enable
   hostname# configure terminal
   ```

2. Begin the upgrade:

   ```
   hostname (config) # ipmi firmware update latest
   ```

3. Confirm the upgrade:

   ```
   hostname (config) # show ipmi
   ```

If the upgrade fails, try the steps again.

If IPMI functions are not fully restored, perform a full power cycle (cold shutdown) on the appliance:

1. Stop the reload process:

   ```
   hostname (config)# reload halt
   ```

2. Disconnect all power cables for 2 minutes.
3. After 2 minutes, reconnect power cables and restart the appliance.

To upgrade the BIOS to version 1.9:

1. Go to CLI configuration mode.

   ```
   hostname> enable
   hostname# configure terminal
   ```

2. Begin the upgrade:

   ```
   hostname (config) # system bios firmware update latest
   ```

   CAUTION! Do not shut down or remove power from the appliance during the upgrade.

3. Confirm the upgrade:

   ```
   hostname (config) # show system bios
   ```

4. Stop the reload process:

   ```
   hostname (config) # reload halt
   ```

5. Disconnect all power cables for 2 minutes.
6. After 2 minutes, reconnect power cables and restart the appliance.

Enabling Access to Intel Context

Advanced Threat Intelligence (ATI) is a cloud-based data collection and threat intelligence distribution feature that provides actionable information about MVX-verified events on appliances. The threat intelligence tells you who is the threat actor behind an attack, what has been targeted or breached, and (if known) how to mitigate the threat. The FireEye Research Labs team continually uploads the latest threat intelligence to the FireEye Dynamic Threat Intelligence (DTI) cloud. When an MVX-verified event triggers an alert, the appliance queries the DTI server for threat intelligence and stores the additional information in its database. When you display an ATI alert, the alert details include the threat intelligence.

Appliances now need access to the Amazon Web Services (AWS) cloud for ATI communication. The intel context service is hosted in multiple AWS regions and resolves to multiple IP addresses based on geographic location. To determine the IP addresses for your location, go to https://dnschecker.org/#A/context.fireeye.com. See the AWS IP address range documentation for information about whitelisting the IP addresses.

What's New

This section describes new features in the FireEye Central Management release 9.1.0.

Improved SmartVision Support

1. You can now enable notifications for SmartVision alerts using the Web UI.
2. SmartVision alert reports can now be generated in both CSV format and PDF format with a single click.

Custom Dashboard Enhancements

The following customization features are available:

- Widgets are categorized as Analysis, Operational, or Detection. Use the dropdown menu on the FireEye Dashboard to filter widgets on the selected category. You can create dashboards that display all widgets in the selected category.
- The Recent Alerts (25) widget shows a table of the 25 most recent alerts. You can view a particular type of alert or all alerts. Click on an alert to see more information.
- The Asymmetric Traffic widget shows a graph of asymmetric traffic flow over the last day or past week.
- You can generate and schedule dashboard reports which contain data from all the widgets on the dashboard. The allowed formats are CSV, JSON, and XML.
- The Scan Count per Storage widget displays the number of scans per storage type.
- The Scan Count per Scan Status widget displays the number of completed, configured, paused, running, or aborted scans.
- The Scan Count per Scan Type widget displays the number of scans per scan type.

Web UI Riskware Alerts for File Protect

File Protect appliances and Central Management appliances managing a File Protect appliance now support riskware alerts on the Web UI. The following features have been

added:

- You can download an XML file of riskware alerts.
- A Riskware Alerts count has been added to the Alerts Summary widget.
- A Riskware Alert count badge has been added for each scan in the **Scans** page.
- In the **Settings > Riskware Policy** page, you can generate an alert or quarantine an item flagged as riskware.
- In the **Alerts** page, you can filter the table to show only riskware alerts.

Trend Alerts Covering Traffic Anomalies

You can enable quicker detection, diagnosis and add the ability to troubleshoot issues in your network. This feature provides deeper insight and visualization of asymmetric traffic, traffic pattern changes, and inactivity.

Reports for Riskware Alerts

You can generate and download riskware details reports for different riskware alerts for a specified time frame. The following riskware alerts are supported:

- Riskware-Callback
- Riskware-Object
- Riskware-Infection
- All

"Blocked" Badge for Riskware Alerts

The Riskware Alerts page now displays a "Blocked" to indicate an alert has been blocked.

Migration of Python Scripts from Python 2.75 to Python 3.6

Python 2.x is no longer supported. Scripts are migrated from Python 2.75 to Python 3.6.

Limiting the Number of Backup Files on Your Appliance

For **Local Backups**, you can specify a limit to the number of backup files that can be stored on your appliance. When the number of backup files on your appliance reaches the specified limit, you need to delete old backups to continue performing local backups. For details, see the "Limiting the Number of Backup Files on Your Appliance" section in *Central Management Administration Guide*.

IPv6 Support for the IPMI Interface

For CM 7500 and CM 9500 appliances, you can configure IPv6 addresses for the IPMI interface. For details, see the "Configuring IPv6 Addresses for the IPMI Interface" section in *Central Management Administration Guide*.

IPv6 Support for Central Management Peering

The Central Management peering service is now IPV6 capable.

Updates to the FireEye Web UI

The following aspects of the UI have been updated to be consistent across FireEye products and to improve usability:

- Header and Footer Section
- About Page
- IPS Page section (IPS Events, Custom Rules, Configure, and IPS Policy Sync Pages)

CLI Commands Search Tool

You can search for CLI commands available in your appliance with text filters and match commands with regular expressions in the CLI.

Log Management

The following changes have been made to log management:

- You can tag and remove system internal audit messages from the audit log file.
- You can archive audit logs and login history logs periodically, when they reach a specified file size, or when they reach a specified percentage of the disk size.
- You can generate an Everything log and upload this to technical support.
- The Operator user role can show, delete, and upload logs.

Configuring Central Management High Availability Pairs Without Additional HA License

It is now easier to provision and configure Central Management High Availability (HA) pairs without an additional HA license by enabling HA mode on the appliance.

SOCKS5 Tunnelling Support for Managed Appliance and Central Management Appliance Communications

A SOCKS proxy connection from managed appliances provides information exchange between devices deployed in multiple networks. You can connect multiple managed appliances to a single SOCKS proxy server.

Adding Managed Appliances to Central Management Using Jump-Start Wizard

An option to integrate with Central Management is now available in a managed appliance CLI configuration jump-start wizard. The Web UI wizard now includes SSH key options, and indicates when an SSH key has been configured in the client.

For more information about adding a managed appliance to Central Management using the Jump-Start wizard, see the *Central Management Administration Guide.*

Central Management Supports Shifting IP Addresses for Managed Appliances Connecting Through NAT

You can now use the Web UI to accommodate managed appliances that use shifting IP addresses. See the options on the new Appliance Connections tab.

Access to Troubleshooting Commands from the CLI

You can use the following troubleshooting commands without requesting a Restricted Shell License:

- `dig`
- `ldapsearch`
- `openssl s_client`

SAML Login Redirected Automatically

if the Web policy is set to required-force, users will be redirected from the FireEye appliances login page to the IDP login page automatically without clicking the sign-in link.

For more information, see the *FireEye System Security Guide*.

New Filters Available on Central Management Managing a Connected Email Security — Server Edition Appliance

On a Central Management appliance that manages an Email Security — Server Edition appliance, you can filter alerts in the Alerts > eAlerts > Alerts page by URL, Tag Name, or Tag Value.

New Filter Available on Central Management Managing a Connected File Protect Appliance

On a Central Management that manages a File Protect appliance, when you click Files Infected in the Alerts Summary widget, the Alerts page displays the number of infected files.

Monitoring Appliance Performance

You can use the `show perfmon` CLI commands to view and create a log of system performance statistics.

For more infromation, see the *CLI Command Reference*.

New and Modified APIs

New API endpoints are available for Network Security, Email Security — Server Edition, File Protect, and Malware Analysis.

For details, see the *FireEye API Reference Guide*.

Web UI Riskware Alerts for Malware Analysis

Malware Analysis appliances and Central Management appliances managing a Malware Analysis appliance now support riskware alerts on the Web UI. The following features have been added:

- You can download an XML file of riskware alerts.
- A Riskware Alerts count has been added to the Alerts Summary widget.
- The File Analysis Statistics widget displays the types of files submitted for analysis.
- The Top (10) Signatures by Alerts Count displays the most common signatures submitted for analysis.

HomeNet Configuration Enhancements

You can add multiple HomeNet IP addresses in the Network Security and Central Management appliance. You can perform the following functions:

- Add one or more HomeNet IP addresses.
- Delete one or more HomeNet IP addresses.
- Apply HomeNet IP addresses to the BOTT engine.
- Upload .CSV and .TXT files containing IP addresses entries. Separate addresses with newline characters.

Content Source Updates When DTI Network Is Switched

When you switch from a cloud URL to a static cloud URL for DTI connectivity, the following content sources for each service are updated:

- Download
- Enrollment
- FAUDE
- Global
- Cache
- Mil
- Upload
- Virtual

Interface Artifacts Information in the File Protect and Central Management Appliances

In the Alerts page, you can view a description of these artifacts:

- Malicious Alerts
- OS Change Graph and Table

- Macro Samples
- FireEye Labs Obfuscated String Solver (FLOSS)
- Event and FAUDE Detection Screenshots
- PE Parser, Object File Hash, HEX files, and Mitre Attack Mapping

SAML Authentication Update for Roles

You can prevent users logging into the appliance using SAML authentication for specific local user roles.

Central Management HA Details on Failovers

The Central Management appliance provides easier understanding and troubleshooting of CMS HA failovers:

- Network outage
- Appliance reboot
- Random packet drop between the two HA nodes
- Manual failover
- Node shutdown
- Resource agent time-out

Other Enhancements

- You can now perform full backups more quickly because unnecessary core files are not backed up during the backup process.
- The Root Filesystem is cleaned up to retrieve reasonable disk space.
- When a fourth-generation appliance nears its end-of-life, a notification appears under the bell in the top right of the Web UI header. Click the URL on the notification for more details.

New, Modified, or Deprecated CLI Commands

The CLI commands in this section were added, modified, or deprecated for this release.

New Commands

Use the following commands to view and create a log of system performance statistics:

- `show perfmon buddyinfo`

  Displays the fragmentation state of the system memory.
- `show perfmon disksleep`

  Displays processes that are in disk sleep while waiting for a file descriptor. Processes in this state cannot be interrupted or ended.
- `show perfmon disktps`

  Displays the number of input and output requests per second.
- `show perfmon iostat`

  Monitors system input and output processes for devices and partitions.
- `show perfmon iotop`

  Displays the number of active input and output processes.
- `show perfmon iowait`

  Displays the percentage of time that the CPU was idle while the system had an outstanding disk I/O request.
- `show perfmon ldavg`

  Displays the system-wide load average.
- `show perfmon mgmtdfdcount`

  Displays the number of mgmtd open files and displays detailed information if the count is near the warning level.
- `show perfmon mgmtdstack`

  Displays mgmtd user and kernel stack details.
- `show perfmon psmem`

  Displays per-process memory utilization.
- `show perfmon smem`

  Displays proportional set size per-process memory utilization.

Use the following commands to add, delete, apply, and show the HomeNet IP address configurations:

- `[no] homenet ip <CIDR1 CIDR2 CIDR3 ...>`
- `no homenet ip all`

- `homenet apply-update`
- `show homenet`

Use the following commands to enable and use a SOCKS proxy connection:

- `[no ] socksproxy enable`
- `[no ] socksproxy <proxy-id>`
- `socksproxy <proxy-id> address <proxy-address>`
- `[no ]socksproxy <proxy-id> port <proxy-port>`
- `socksproxy <proxy-id> authtype <auth-type>`
- `socksproxy <proxy-id> auth password username <proxy-username>`
- `socksproxy <proxy-id> auth password password <proxy-user-password>`
- `socksproxy <proxy-id> auth ssh-rsa2 username <proxy-username>`
- `socksproxy <proxy-id> auth ssh-rsa2 identity <identityname>`
- `socksproxy <proxy-id> auth ssh-dsa2 username <proxy-username>`
- `socksproxy <proxy-id> auth ssh-dsa2 password <identityname>`
- `show socksproxy`
- `socksproxy <proxy-id> connect`
- `cmc appliance <appliance-id> use-socksproxy <proxy-id>`
- `no cmc appliance <appliance-id> use-socksproxy`

This command restricts SAML authentication for specific user roles:

- `aaa authorization rules rule append tail match-auth-method saml reject-local-user monitor`

Use this command to filter commands available in your appliance using regular expressions:

- `show cli commands matching <FilterText>`
- `show cli commands include-incomplete matching <FilterText>`

The following commands configure IPv6 for the IPMI interface only for CM 7500and CM 9500 appliances:

- `ipmi lan6 ipaddr <IPv6 Address> prefix <1-28>`

  Configures IPv6 address for the IPMI interface.
- `ipmi lan6 dhcp enable`

  Enables DHCP on your network.

The following commands configure a limit to the number of backup files that can be stored on your appliance:

- `backup limit <max-number-of-backups-allowed>`

  Specifies the maximum number of backup files that can be stored on your appliance.
- `backup reset maxcount`

  Resets the custom backup limit to the default value—25.

The following command uploads CM telemetry and statistics to the DTI cloud automatically every three hours:

- `fenet stats-content upload auto default`

The following command automatically deletes the oldest local backup file (when the backup files limit is crossed) and then backs up the appliance:

- `backup profile <profile> to local auto-delete-old`

SFTP and SCP file transfer protocols are disabled by default. To enable them, use the following commands:

- `ssh server services file-transfer scp enable`
- `ssh server services file-transfer sftp enable`

Use the following commands to enable the High Availability (HA) feature:

- `[no] ha enable` enable or disable the HA feature.
- `[no] cms feature ha available` enable or disable the Central Management HA feature.

Use the following command to enable and disable WebSocket protocol support:

- `[no] foxd config protocol websocket enable`

Use the following commands for foxd configuration:

- `[no] foxd config vlan enable`

  Enable or disable foxd vlan support.
- `[no] foxd config postextract enable`

  Enable or disable foxd post-extract support.
- `[no] foxd config protocol <protocol> enable`

  Enable or disable customized foxd configuration, specifying one of the following protocols: `dnp3`, `imap`, `modbus`, `radius`, `socks`, `dns-tcp`, `dns-udp`, `irc`, `krb5`, `mysql`, `pop3`, `rdp`, `smtp`, `ssh`.

Modified Commands

- `aaa authentication saml web policy`

  A new parameter, `required-force`, allows you to enforce SAML authentication redirection.

Deprecated Commands

You can no longer configure daily, hourly, weekly, and monthly schedules for uploading aggregation statistics automatically to the Dynamic Threat Intelligence (DTI) network. The following commands are deprecated:

- `fenet stats-content upload auto daily at <hh:mm>`
- `fenet stats-content upload auto hourly at <mm>`
- `fenet stats-content upload auto monthly on <date> at <hh:mm>`
- `fenet stats-content upload auto weekly every <day> at <hh:mm>`
- `fenet stats-content upload auto none`

You can no longer configure SSL versions TLS 1.0 and TLS 1.1 for DTI network communication. The following commands are deprecated:

- `fenet ssl min-version tls1.0`
- `fenet ssl min-version tls1.1`

The following foxd configuration commands are deprecated and replaced by the new `foxd config*` commands:

- `foxd config custom enable`
- `foxd config custom vlan enable`

Fixed Central Management Issues

The following issues were resolved in the Central Management 9.1.0 Release.

The relevant issue tracking numbers for each item are included in parentheses.

- If a new cluster was created with a new Virtual Execution (VX) node and the VX node was deleted while the cluster was being created, the managing Central Management appliance displayed an “unknown” prompt after it was rebooted. This issue has been resolved. **(CMS-15092)**
- On a Central Management high availability node running Release 8.7.2, the squid process sometimes failed when it attempted to cache an image. This issue has been resolved. **(CMS-15560)**
- A Central Management appliance sometimes failed to send alerts to Helix or a SIEM, causing a backlog of alerts on the Central Management appliance. This issue has been resolved. **(CMS-15644)**
- When an on-premises Central Management appliance was configured in Helix on-premises mode, the setting unexpectedly changed to Helix cloud mode, preventing managed appliances from downloading content from the DTI. This issue has been resolved. **(CMS-15669)**
- When Advanced URL Defense was disabled in the Central Management Web UI, it was sometimes re-enabled automatically on managed Email Security — Server Edition and Virtual Execution appliances. This issue has been resolved. **(CMS-15845)**
- Some low-risk issues detected by automated scanners have been resolved. **(CMS-15862)**
- The femexd process on a Central Management 9400 model remained in a pending state. This issue has been resolved. **(CMS-15944)**
- IPS policy sync matching was improved on a Central Management appliance that managed a Network Security appliance. **(CMS-15946)**
- If the group filter in the CM Web UI was set to Network Security, and then a time filter was specified on the eQuarantine page, the page did not display any quarantined emails. This issue has been resolved. **(CMS-15966)**

- The Monitored Traffic section of the Central Management Dashboard intermittently reported no traffic on a managed Network Security appliance. The graph updated to show the actual traffic after a few minutes. This issue has been resolved. **(CMS-16034)**
- When logs were generated on a Central Management appliance running release 8.7.2, the messages.log file sometimes was not generated. This issue has been resolved. **(CMS-16039)**
- A Cloud Central Management appliance returned incomplete alert data for ETP events. This issue has been resolved. **(CMS-16113)**
- In a Central Management high availability environment, kernel problems occurred intermittently during synchronization. The primary node did not fail over to the secondary node properly. The sync was not completed, and managed appliances were disconnected from the cluster. This issue has been resolved. **(CMSHA-1284, CMSHA-1306)**
- In some circumstances, when a Central Management high availability cluster experienced a split brain condition, the cluster was not shut down as expected although auto-shutdown was enabled. This issue has been resolved. **(CMSHA-1318)**
- If an appliance that was managed by a Central Management high availability cluster stopped responding, the cluster failed over unexpectedly. This issue has been resolved. **(CMSHA-1355)**
- Some configuration changes made in the Web UI were not saved. This issue has been resolved. **(CMSHA-1386)**
- At times, a Central Management high availability cluster did not respond correctly to the ha engine failover command. The secondary node did not take over and neither node became primary. This issue has been resolved. **(CMSHA-1423)**
- The version of Samba was upgraded to 4.10.4-11 to protect against the potential vulnerability outlined in CVE-2018-10858. **(COM-24540)**
- The `email send-test` command returned a segfault error if the SMTP authentication password was not defined. This issue has been resolved. **(COM-25069)**
- Extra space sometimes appeared in syslog output shown in JSON extended format. This issue has been resolved. **(COM-25809)**
- The expat tool was upgraded to version 2.1.0-12 to protect against the potential vulnerability outlined in CVE-2018-20843. **(COM-25958)**
- The Intel nvmupdate utility was added to protect against the potential vulnerability outlined in INTEL-SA-00255. **(COM-26735)**
- Components of jquery were upgraded to protect against known vulnerabilities in JavaScript. This issue has been resolved. **(COM-26783)**

- The version of Apache used caused 403 and 404 page errors to be displayed. This issue has been resolved. **(COM-26802)**
- Rsyslog notifications sent using the UDP protocol sometimes omitted the first packet. This issue has been resolved. **(COM-27181)**
- In some circumstances, the lmsd.snmpapp.conf file could grow very large because new information was appended to its contents instead of overwriting them. This issue has been resolved. **(COM-27251)**
- The `fedb maintenance vacuum` command failed to perform a vacuum on some parts of the fedb database. This issue has been resolved. **(COM-27508, COM-27510)**
- When the message file was rotated, all other logs were rotated and custom log rotation settings were ignored. Smaller log files were purged too often. This issue has been resolved. **(COM-27594)**
- If an email message contained URLs in an attached .ics file, the URLs were not extracted properly and the email was passed as clean. This issue has been resolved. **(COM-27692)**
- Files in the /var/root/tmp directory were not cleaned up properly and old files were retained, consuming disk space. This issue has been resolved. **(COM-27737)**
- On a Network Security appliance running release 8.2.3, the rsyslogd process crashed repeatedly with fatal errors This issue has been resolved. **(COM-28110)**
- Guest images were updated to protect against potential vulnerabilities in the QEMU software emulator. This issue has been resolved. **(COM-28261)**
- It was possible to enter email addresses in an invalid format for recipients of some reports. This issue has been resolved. **(COM-28613)**
- A potential vulnerability in libcURL related to CVE- 2020-8285 has been fixed. **(COM-28427)**
- TLS versions earlier than TLS 1.2 are no longer supported. This issue has been resolved. **(COM-28411)**
- Helix health statistics could not be uploaded using a proxy. This issue has been resolved. **(COM-28554)**
- It was possible to enter license keys that were too long. The maximum length for license keys is now 8192 characters. This issue has been resolved. **(COM-28614)**
- If guest images could not be downloaded, an SNMP "low disk space" alert was displayed regardless of the reason the download failed. This issue has been resolved. **(COM-28826)**
- FireEye appliances are not affected by the OpenSSL vulnerabilities described in CVE-2021-3449 and CVE-2021-3450. **(COM-28835)**

- FireEye appliances are not affected by the nodejs-netmask vulnerability described in CVE-2021-28918. **(COM-28836, COM-28871)**
- A long scan running on a File Protect appliance became stuck in the "aborting" state and could not be canceled or restarted. This issue has been resolved. **(COM-28855)**
- The libssh2 package was upgraded to protect against the potential vulnerability described in CVE-2019-3855. **(COM-28943)**
- In an on-premises Endpoint Security server, the httpd process remained in a pending state and prevented access via the Web UI because the directory was filled with core dump files that were not removed. This issue has been resolved. **(COM-29056)**
- Following a delta update of security content, the output of the `show fenet security-content status` command reported that a full update had been performed. This issue has been resolved. **(FNET-1942)**
- After an appliance was successfully upgraded and reloaded, the output of the show fenet image status command continued to state that a reload was required. This issue has been resolved. **(FNET-1951)**

Known Central Management Issues

The following issues are known in Central Management release 9.1.0.

The relevant issue tracking numbers for each item are included in parentheses.

- When a cluster is created on a Central Management appliance, disconnected from that appliance, and then added to another Central Management appliance, the cluster group is not created on the second appliance and utilization cannot be viewed. As a workaround, delete the cluster from the second Central Management appliance and then recreate it. **(CMS-15613)**
- After an upgrade from release 8.6.0 to release 9.1.0, restoring a backup on a Central Management appliance causes mgmtd.WARNING and java.WARNING messages to appear in the log. **(CMS-15651)**
- The Central Management appliance does not allow an Operator user to add a domain whitelist from the Settings > Appliance Settings > Whitelists page. **(CMS-16004)**
- In the Web UI of 9.1.0 Central Management appliances that manage Network Security appliances, the YARA rules tab is not accessible to access group users mapped with the `match-yara-rules-access` rule. **(CMS-16031)**
- Connecting an appliance in the Central Management CLI with a SOCKS proxy using the command `cmc appliance <ApplianceName> connection connect` sometimes fails. **(CMS-16092)**
- IPS policy synchronization fails on a 9.0.x version Network Security appliance that is managed by a 9.1.0 Central Management appliance. **(CMS-16112)**
- On Central Management appliances managing appliances that use the 9.1.0 release, no events appear for test-fires in the Alerts tab of the Web UI. **(CMS-16158)**
- After an upgrade from 9.0.3 to 9.1.0, Central Management appliances with managed Network Security appliances show a IPMI warning: `sensor command returned nothing`. (**CMS-16298)**
- The Central Management high availability cluster is unstable while a node is inserted. **(CMSHA-1428)**

- In a high availability environment, changing the host name via Central Management renames a cluster with both the new hostname and the old hostname. To resolve this issue, run the `reset cluster-engine` command. **(CMSHA-1434)**
- In the Web UI, the numbers for total malicious email, malicious URLs, and malicious attachments displayed on the Dashboard do not match those displayed on the Alerts page. **(COM-27715)**
- The command `fenotify integ helix enable` is required to be run on appliances managed by a Central Management appliance to integrate with Helix. These appliances cannot use Helix Connect as they are required to proxy through the Central Management appliance. **(COM-27793)**
- In the IPS Custom Rules page of the Web UI, the export rules feature fails if the page is idle. **(WEBUI-13784)**
- In the About tab of the Web UI, accepting "improve detection" via the bell notification causes a routing error. **(WEBUI-14031)**

Technical Support

For technical support, contact FireEye through the Support portal:

https://csportal.fireeye.com

Documentation

Documentation for all FireEye products is available on the FireEye Documentation Portal (login required):

https://docs.fireeye.com/

FireEye, Inc. | 601 McCarthy Blvd. | Milpitas, CA | 1.408.321.6300 | 1.877.FIREEYE | www.fireeye.com