Resolved Issues

For devices running or hosted on a non-Firepower appliance (for example, ASA OS or FXOS), resolving an issue may require that you update the operating system *in addition to* Firepower. We recommend you update to the latest **supported** version.

The following defects are resolved in Version 6.2.0:

Caveat ID Number	Description
CSCuw70987, CSCux50957, CSCux86317	Resolved multiple vulnerabilities within the third party Open SSH, as described in CVE-2015-5600, CVE-2015-6565, CVE-2016-0777, and CVE-2016-0778.
CSCuw88390, CSCuw88396, CSCuw89094	Addressed a cross-site scripting (XSS) vulnerability, as described in CVE-2015-6363 and CVE-2016-1294.
CSCux41304, CSCuz52366, CSCvb24543, CSCvb48536	Addressed multiple vulnerabilities that generated denial of service in OpenSSL, as described in CVE-2015-3194, CVE-2015-3195, CVE-2015-3196, CVE-2016-2105, CVE-2016-2106 CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6305, CVE-2016-6306 CVE-2016-6307 CVE-2016-6308 CVE-2016-6309 CVE-2016-7052 CVE-2015-3194, CVE-2015-3195 and CVE-2015-3196.
CSCux42288	Addressed a vulnerability issue in the third party Java, as described in CVE-2015-6420.
CSCux90163	Resolved a vulnerability where a user without Admin without privileges could delete other users' scheduled tasks.
CSCuy32284	Addressed a vulnerability in the third party GNU C Library, as described in CVE-2015-7547.
CSCuz52939, CSCvb24561, CSCvb24562	Addressed multiple vulnerabilities in the third party product Libxml2, as described in CVE-2016-2073, CVE-2016-444, and CVE-2016-4448.
CSCuz92632	Addressed multiple vulnerabilities in the third party product NTP, as described in CVE-2016-4953, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956, and CVE-2016-4957.

Caveat ID Number	Description
CSCvb24566, CSCvb24564 CSCuz52935	Address multiple vulnerabilities in the Libarchive, as described in CVE-2016-1541, CVE-2016-5844, and CVE-2016-6250.
CSCuu96447	In some cases, if you deleted the permanent license from the Licenses page **System** > **Licenses**, the Device Management page **Devices** > **Device Management** did not display **Unlicensed** for devices the permanent license was deleted from when it should have, and policy deploy would fail.
CSCux64898	In some cases, if you deployed an access control policy with the default action set to **Block** and executed the **configure network management-interface disable-event-channel** CLI command, Firepower continued to generate intrusion and connection events when it should not have.
CSCux78211	Resolved an issue where, if an ASA FirePOWER module in high availability experienced a partial failure, the device did not failover when it should have.
CSCux91934	Resolved an issue where, if you deployed an SSL policy configured with a rule associated with an expired SSL certificate, Firepower used an incorrect SSL rule.
CSCuy28088	Cannot apply FP8130-CTRL-LIC to AMP8050.
CSCuy49371	If you clicked **Create Email Alert** on the Alerts page **Policies** > **Actions** > **Alerts** and enabled **Retrospective Events configuration** on the Advanced Malware Protection Alerts tab, then saved and applied, the email alerts generated by Firepower when the alert was triggered were truncated. Emails should not have been truncated.
CSCuy51566	If you updated a Firepower Management Center from Version 5.4.x to Version 6.0.0 or later and created a new sub domain and deployed a network discovery policy, you could not delete any objects or object groups referenced by the network discovery policy in the global domain.
CSCuy57756	In some cases, if you broke a Firepower Threat Defense high availability pair, one of the devices in the pair stayed in standalone mode and Firepower could not recreate the high availability pair.
CSCuy67210	Not able to disable notifications on the Firesight manager Web interface.
CSCuy68648	Resolved an issue where, if you added a security zone on a Firepower Management Center running Version 5.4.0 or later and updated Firepower to Version 6.0.0 or later and deleted the security zone, Firepower generated an **Object deletion restricted. Remove object from the following: Access control policies** error even if the security zone was not referenced within a rule.
CSCuy83201	Fatal errors on applying policy from 6.0.0.1 with different vulnerability database.
CSCuz17315	Resolved an issue where Firepower generated erroneous **Error found during SSL flow after server certificate** messages for evicted SSL flows.
CSCuz17723	Firepower 9300 devices' high availability status is displayed incorrectly/inconsistent in the Firepower Management Center.

Caveat ID Number	Description
CSCuz24872	Original Client IP does not populate for dropped events when inline normalization enabled.
CSCuz46366	Firepower incorrectly allowed you configure sandbox file sizes from 0 MB to 100 MB on the Files and Malware Settings section on the Advanced tab of the access control editor. Firepower only supports capturing files as large as 10 MB. If you configured the sandbox environment to a file size larger than 10 MB, Firepower did not capture the file.
CSCuz49023	Resolved an issue where despite configuration of impact flag alerting for an eStreamer client, Firepower did not stream impact flag data.
CSCuz54417	If you deployed an SSL policy containing application rule conditions for **SMTPS**, **POP3S**, and **IMAPS** traffic, Firepower might have incorrectly displayed Unknown as the application protocol in the Connection Events page **Analysis** > **Connections** > **Events**.
CSCuz78239	DLL-Load vulnerability in Snort on Windows platforms.
CSCuz92255	Resolved an issue where, if you tested the default storage type on the Remote Stage Device section of the Configuration page **System** > **Configuration**, Firepower incorrectly generated a **Please enter valid host. Please enter a valid Directory path.** error message.
CSCuz92983	Policy deployment fails with mode 10 Gbit Full-Duplex for lag interface.
CSCuz94444	Resolved an issue where the associated client incorrectly rejected resigned certificates for Apple related products and you could not log into iTunes.
CSCuz95008	Resolved an issue where, if you requested pre 6.0.0 metadata from a Firepower Management Center with eStreamer running Version 6.0.0. or later, Firepower incorrectly sent the **userID** field to the eStreamer client instead of the configured LDAP username.
CSCuz99677	Resolved an issue where, if you created a new user with an administrator role and deployed configuration, Firepower incorrectly displayed the default admin user as the user deploying the configuration instead of the newly created user.
CSCva00234	Resolved an issue where policy comparison did not include the high availability health modules when it should have.
CSCva01674	sfestreamer crashes when we have 4 management interfaces on Firepower Management Center.
CSCva12481	Disk manager marks conn-unified as deleted.
CSCva28854	Under rare conditions, when 7000 and 8000 Series devices where firstboot policy apply failed, file handles are depleted on the device which caused health/hardware alarms and a variety of malfunctions.

Caveat ID Number	Description
CSCva29636	Resolved an issue where, if you configure network management for a Firepower Threat Defense virtual device, the console incorrectly provided an HTTPS address to complete the installation when it should not have.
CSCva37443	If your ASA configuration file contained an invalid ICMP service object, the ASA-to-Firepower Threat Defense migration tool failed, but did not log adequate information to troubleshooting logs. Migration no longer fails under this condition. Instead, the tool excludes the invalid ICMP objects from the conversion, converts the related ASA access rules to disabled Firepower Threat Defense rules, and adds a comment to the rules describing the unsupported case.
CSCva38608	Resolved an issue where SHA1 signed certificate with a modern browser and Firepower generated untrusted certificate errors for modern browser.
CSCva41164	Version 6.2.0 does not support access control policy names including the **$** character.
CSCva47456	Resolved an issue where, if Firepower requested a URL lookup and the cloud did not immediately return a URL category, the cached request incorrectly remained marked as **Pending** instead of updating the URL type to **Uncategorzied**.
CSCva49869	Report generation did not give a failed message, continues in queue for week.
CSCva51022	If you deployed a pair of network object groups to a Firepower Threat Defense high availability pair and the network object group IP addresses on either the active and standby device overlapped with the IP addresses on the other device within the pair, deployment failed and Firepower generated a Deployment failed due to configuration error message in the Message Center.
CSCva51662	Resolved an issue where, if you clicked **Launch Readiness Check** while another readiness check is in the queue and closed the dialog window, Firepower incorrectly started a new readiness check task .
CSCva57174	On a Firepower Threat Defense Virtual with RIP and redistribution configured, even if you disabled RIP and redeployed, the device continued to use RIP.
CSCva58269	Resolved an issue where, if you created alerts associated with a domain and then deleted the domain, Firepower did not remove the alerts from the database when it should have.
CSCva58393	User is able to apply smart licenses on AWS HB device.
CSCva58411	Resolved an issue where, if you added smart licenses to a Firepower Threat Defense high availability pair, the smart licensing widget on the dashboard page did not load.
CSCva59135	The ASA-to-Firepower Threat Defense migration tool can convert only one ASA configuration file at a time. If you started a conversion while a conversion task was in progress, Firepower displayed an **Error 500 Internal server** error message. Firepower now displays a warning message that a migration is already in progress.

Caveat ID Number	Description
CSCva63604	Resolved an issue where, if a security module on a Firepower Threat Defense cluster with an access control policy containing more than 10,000 rules reloaded, the security module failed to re-join the cluster and generated a **All data interfaces have been shutdown due to clustering being disabled. To recover either enable clustering or remove cluster group configuration** warning.
CSCva67943	Resolved an issue where, if you enabled common criteria (CC) mode on an appliance for security certifications compliance and the syslog server certificate did not contain serverAuth, Firepower incorrectly passed connections to the syslog server when they should have failed.
CSCva72899	Access control policy report fails if category has span across 50 rules.
CSCva81548	Improved configuration deployment performance.
CSCva82945	The Interfaces tab of the device management page for a Firepower Threat Defense device now displays the current status for interfaces on the device.
CSCva89328	Resolved an issue where, if you deployed an intrusion rule containing an AppID web application condition and a managed device experienced a high volume of traffic containing an excessive amount of similar connection types that did not apply to the AppID application, the application detection process took more time than it normally should and caused latency for other traffic matches.
CSCva89342	If you created an ASA Firepower module high available pair configured for multi-context mode and deployed one or more security zone from the managing Firepower Management Center, then the standby ASA Firepower module within the pair restarted, the standby ASA Firepower module incorrectly removed all security zones and interfaces.
CSCva93408, CSCva93158	Improved the RPC decoder.
CSCva99998	Resolved an issue where Firepower did not restrict read-only users from editing the blacklist page when it should have.
CSCvb02417	Adaptive profiling performance scales badly in some cases.
CSCvb02846	Resolved a rare issue where, if you switched Firepower Management Center high availability peers twice and viewed the Smart Licenses page **System** > **Licenses** > **Licenses** > **Smart Licenses**, the table of devices and any edit windows failed to load.
CSCvb05694	Resolved an issue where, if you deployed an SSL policy and traffic with an HTTP tunnel matched the SSL policy, Firepower dropped some traffic and experienced high CPU use and overall latency.
CSCvb08840	Resolved an issue where, if you enabled automated intrusion rule updates for an ASA Firepower module managed by ASDM, and the device simultaneously deployed automated deployments, the device experienced issues.

Caveat ID Number	Description
CSCvb11574	Resolved an issue where, if you deployed an access control policy containing a custom application detector and deleted the application detector, Firepower did not generate a warning that the application detector must be removed from the access control policy prior to deletion.
CSCvb11642	Resolved an issue where, if you created a network discovery policy configured to detect hosts and a correlation policy containing a rule set to trigger if discovery event occurs and the OS information for a host has changed, then added a condition for if OS name is unknown and added a remediation Nmap scan, discovery events matching the rules did not generated corresponding Nmap scans.
CSCvb11931	Resolved an issue where, if Firepower experienced an issue processing the first session of SMTP traffic between a client and an SMTP server, Firepower did not correctly identify the subsequent SMTP sessions as SMTP for the client-server pair and displayed Unknown in the Application Protocol column of the Connection Events page **Analysis** > **Connections** > **Events**.
CSCvb12453	Resolved an issue where, if you enabled common criteria (CC) mode on an appliance for security certifications compliance and the syslog server certificate did not contain host name matching the name of the server, connections to the syslog server incorrectly passed when they should have failed.
CSCvb12791	Resolved an issue where, if you enabled Common Criteria (CC) mode on an appliance for security certifications compliance and the syslog server certificate and/or intermediate certificate(s) have been revoked, Firepower incorrectly established a TLS connection with the syslog server without checking the revocation status.
CSCvb14402	Traffic by Initiator Report for User Renders No Output.
CSCvb19366	Cisco Firepower Management Center Information Disclosure Vulnerability.
CSCvb19716	Resolved an issue where Firepower Management Center high availability synchronization failed if the total size of the database files and logs totaled more than 4GB.
CSCvb20859	Intermittently, if the ASA-to-Firepower Threat Defense migration tool could not migrate an ASA configuration because the access control list was not applied via a valid access-group command, Firepower did not complete internal operations related to that migration, and you could not start another migration.
CSCvb24378	You can now enable or disable default inspection with the command line interface on a Firepower Threat Defense device using **configure inspection <inspection_name> enable|disable**.
CSCvb24768	Resolved an issue where, in some cases, if you updated a system containing at least one security zone to Version 6.1 or later, the Interfaces page **Devices** > **Interfaces** might incorrectly displayed the security zone state as **Unknown** .
CSCvb24807	In rare cases, after you updated the Firepower Management Center to Version 6.10, the dynamic analysis page **AMP** > **AMP Management** would not load.

Caveat ID Number	Description
CSCvb25963	Resolved an issue where, if you formed a Firepower 4100 series series or Firepower 9300 high availability pair with devices containing named interfaces and assigned a portchannel from the FXOS chassis manager, then edited the Interfaces tab of the high availability pair listed on the Device Management page **Devices** > **Device Management** and saved, Firepower did not include the interfaces created for the high availability pair when it should and, in some cases, deployment failed.
CSCvb26266	Resolved an issue where, if you enabled captive portal on a system and updated to Version 6.1.0, captive portal did not work.
CSCvb28158	Workflow set with User Preferences not honored by Search Constraints.
CSCvb28202	False warnings in database Integrity Check for PlatformSettings object.
CSCvb32484	Upgrade to 6.1 fails at 600_schema/000_install_csm.sh.
CSCvb32873	Cannot create new Application Filter Objects 6.1 on ASA managed by ASDM.
CSCvb35499	Resolved an issue where, in some cases, if you updated a system from Version 6.1.0 to Version 6.1.0.x, the update failed.
CSCvb35861	Resolved an issue where, if you created a high availability pair and synchronization requests overload the Tasks tab in the Message Center, Firepower experienced disk space issues and intermittent login issues.
CSCvb36645	Resolved an issue where, if incoming HTTP, TCP, or SSH traffic did not contain an SGT value in the header, traffic matched against the default access control policy instead of any other configured policy.
CSCvb36847	Event QoS in legacy mode does not have an entry for interface stats.
CSCvb39325	Resolved an issue where incoming HTTP and HTTPS traffic containing XFF fields caused system issues.
CSCvb39435	If you updated Firepower from a version earlier than Version 6.1.0 to Version 6.1.0 and immediately exported the access control policy, then imported the policy, importing the access control policy failed.
CSCvb40344	If you deployed a file policy to a device with an excessive amount of endpoints configured, Firepower experienced high CPU and memory use. As a workaround, you could redeploy configuration.
CSCvb41047	Resolved an issue where Firepower generated an incorrect **Health monitoring running behind schedule** health warning if the Firepower Management Center did not receive any health events from registered devices.
CSCvb42559	Firepower Management Center Smart Licensing bypasses Proxy Configuration when in evaluation mode.
CSCvb43868	Upgrade failing for v6.0.1 at 600_schema/000_install_csm.sh.
CSCvb44812	Resolved an issue where Firepower 4100 series series devices generated excessive logging and experienced storage space issues.

Caveat ID Number	Description
CSCvb44268	Resolved an issue where the Appliance Status widget did not load if you had 400 or more devices attached to a Firepower Management Center.
CSCvb46146	If updating Firepower failed and you attempted to update to a different version from the one that failed without resolving the original failure, the new install also failed and could cause Firepower to become unrecoverable.
CSCvb46555	Resolved an issue where, if you enabled **Safe Search** in an access control policy and deployed, Firepower incorrectly generated **Primary Detection Engine Exiting** health alerts.
CSCvb47847	Resolved an issue where, if you updated a system from Version 6.0.1.1 or later to Version 6.1.0, Firepower experienced a variety of issues such as update failure or Firepower Management Center login failure.
CSCvb51077	Resolved an issue where, if you added a remediation as a response to a rule in a correlation policy on a Firepower Management Center and created a high availability pair, then switch high availability peers, the new active Firepower Management Center did not correctly synchronize the correlation policy and the remediation experienced issues.
CSCvb52057	Resolved an issue where, if you deployed an access control policy containing rules with **Safe Search** enabled, some websites experienced latency when loading.
CSCvb57521	Firepower Management Center/FTD - Multiple default routes with same metric or gateway exists.
CSCvb57747	Deploy during intrusion rule update install may cause all subsequent policy applies to fail.
CSCvb60088	FTD policy deployment fails with Syslog Event class **All**.
CSCvb61055	Security Intelligence synchronization failure results in disk becoming full.
CSCvb61156	Resolved an issue where, if a Firepower Management Center running Version 6.1.0 managed a device running a version earlier than Version 6.1.0, Firepower did not generate any new discovery events and removed the network map several days after the Firepower Management Center updated to Version 6.1.0.
CSCvb61480	In some cases, if Firepower processed SIP packets, traffic containing voice or video content might have appeared distorted or experienced latency.
CSCvb61836	Resolved an issue where Firepower logged extraneous policy information during deployment and, in some cases, deploying large policies failed.
CSCvb65648	Resolved an issue where, if you deployed an access control policy containing an identity policy that referenced a realm or access control rules containing groups or users from the realm and you deleted the realm, Firepower incorrectly generated a **System defined Objects cannot be Altered. Please use a different Object** error and you could not edit the access control policy.

Caveat ID Number	Description
CSCvb66591	If you configured a realm for an Active Directory (AD) server to download users and groups, then created a Firepower Management Center high availability pair and the downloads contained large amounts of users and groups, Firepower Management Center high availability registration failed.
CSCvb67568	Resolved a rare issue where, if you created a realm and deployed an access control policy containing rules, then clicked **Download users and groups** and configured a User Agent connection, the user to group mapping became incorrect and access control rules using groups did not match when it should.
CSCvb68226	SFR upgrade to 6.1 causes constant failover between ASA FirePOWER module high availability pair.
CSCvb69742	6.0.0 pre install 5.4.0.999 nfp kernel modules fail to unload followed by outage.
CSCvb69906	Intermittently, if you created a realm and deployed an access control policy containing rules, then downloaded users and groups (including scheduled downloads), the user-to-group mapping could become incorrect, and access control rules using groups might not have matched when they should have.
CSCvb70125	Resolved an issue where policy deploy failed if you configured captive portal on a Firepower Management Center then updated the Firepower Management Center and its managed devices, then tried to redeploy.
CSCvb74873	If you enabled SMB File Inspection in a file policy and deployed to a device managed by theFirepower Management Center, Firepower generated **Primary detection engine exited unexpectedly** warning messages, and Firepower could experience issues.
CSCvb75591	If you deployed a DNS rule with a blacklist action containing a Security Intelligence DNS feed, Firepower did not send the Security Intelligence events to the external syslog if one was configured.
CSCvb78786	Firepower ignored security zone constraints on network discovery rules if the network discovery policy contained rules constrained by zones that included interfaces from multiple devices. This condition was present if the rules used single zones with interfaces from multiple devices (for example, Zone 1 included interfaces from Device 1 and Device 2) or multiple rules used different zones (for example if Rule 1 used Zone 1, which included interfaces from Device 1, and Rule 2 used Zone 2, which included interfaces from Device 2).
CSCvb79079	Resolved an issue where, if you added a syslog alert to an access control rule and deployed on an ASA FirePOWER module managed by ASDM, the device incorrectly generated excessive logging from prefilter policies.
CSCvb80872	Resolved an issue where, in some cases, updating a system to Version 6.1.0 and deploying to a registered device generated a **Deployment failed in policy and object collection. If problem persists after retrying, contact TAC** error message.
CSCvb88561	Resolved an issue where, if Firepower processed HTTP traffic containing XFF headers, Firepower experienced issues and generated erroneous detection engine health warnings.

Caveat ID Number	Description
CSCvb91730	Attempting to change copper SFP interface type (inline/switched/routed) results in error.
CSCvb91613	Snort cores after reload when processing XFF addresses.
CSCvb94411	In some cases, if you deployed an SSL policy containing an SSL rule with the action set to **Do Not Decrypt** placed above an SSL rule with the action set to **Decrypt - Resign**, Firepower incorrectly identified the sessions as undecryptable and matched against the wrong rule with an undecryptable action instead of the correct rule.
CSCvb97742	7000 and 8000 Series devices with low memory could experience a traffic outage and not recover.
CSCvc05323	Resolved an issue where snort restarts caused Firepower to generate extraneous **NGFW Rule Engine Failed to write connection event** log messages.
CSCvc08057	Resolved an issue where FTD devices experienced Snort cores while performing QoS rate limiting on destination interface objects.
CSCvc08912	No input validation on FTD Platform Setting syslog Logging Filter.
CSCvc09761	Cannot delete multiple rules at a time from ASA migrated Prefilter Policies.
CSCvc10655	Resolved an issue where deploying policies to a FTD device failed after updating to a new Firepower version.
CSCvc14561	Resolved an issue where the Firepower Management Center web interface was not available after enabling compliance mode.
CSCvc26880	Resolved an issue where, if a Firepower 8350 device or AMP8350 device produced an unusually large stream of messages on the serial port console or, if you enabled it, the Lights-out Management (LOM) console, the device became unresponsive.
CSCvc30591	eStreamer should use correct datastore for user identity mapping.
CSCvc31852	Resolved an issue where the Firepower Management Center Tasks tab displayed an incorrect amount of time taken for policy deployment.
CSCvc36047	Having **0** at the object service PING service icmp echo 0 causes migration to fail.
CSCvc37923	Resolved an issue where Firepower did not recover from a disk write error caused by disk full even after the disk full issue was resolved, causing excessive logging.
CSCvc37927	Import fails with duplicate object name when the object names differs by case only.
CSCvc44398	URL not extracted from reassembled requests.
CSCvc49641	Snort process segfaults processing traffic in firewall.
CSCvc49789	OptimizeTables.pl always fails on 6.1.0.
CSCvc53628	Available Ports tab hangs when editing prefilter rule ports.

Caveat ID Number	Description
CSCvc54134	Resolved an issue where, when a FTD high availability pair simultaneously rebooted, the pair continuously rebooted until the failover cable was removed.
CSCvc55170	Firepower Management Center login stops working if **resume sync** is selected after upgrade.
CSCvc58398	Firepower Management Center warnings needed during high availability configuration that configuration on the standby Firepower Management Center will be wiped.
CSCvd78303	Version 6.2.0-363 resolved an issue where the FTD device running Version 6.1.0.1 or Version 6.1.0.2 stopped passing traffic after 213 days of uptime and experienced a range of issues from limited connectivity to a traffic outage.