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.*x*:

Issues Resolved in Version 6.2.0.6

The following table addresses resolved caveats at the time of publication of these release notes. If you have a Cisco support contract, use the following dynamic queries for an updated list of resolved caveats, run the provided query in the Bug Search Tool:

- Resolved Firepower Management Center caveats in Version 6.2.0.6
- Resolved Firepower Management Center Virtual caveats in Version 6.2.0.6
- Resolved ASAFirePOWER caveats in Version 9.7.x

Caveat ID Number	Description
CSCuy57310	Cisco Adaptive Security Appliance Traffic Flow Confidentiality Denial of Service Vulnerability
CSCvc91092	Cisco FireSIGHT System Software Arbitrary Code Execution Vulnerability
CSCvd02391	Enabling URL filtering license for Firepower Threat Defense breaks the smart license.
CSCvd76821	**tcp-options md5 allow** is pushed to slave units as tcp-options md5 clear
CSCvd96108	Traceback in thread name `DATAPATH` due to lan to lan VPN

Caveat ID Number	Description
CSCve31387	No CPU alert on 8000 Series, when snort is overwhelmed.
CSCve87945	Cannot install new https certificate
CSCve97046	`threat_name` table prune cannot keep up with insertion
CSCvf53734	access control rules and Categories duplication on Firepower Management Center UI
CSCvf56533	Cannot re-register Firepower 9300 cluster to a different Firepower Management Center
CSCvf64831	Firepower Management Center reports incorrect IPv6 addresses and ports
CSCvg00565	ASA crashes in `glib/g_slice` when do **debug menu** self testing
CSCvg05368	Upon joining cluster slave unit generates ASA-3-202010: NAT/PAT pool exhausted for all PAT'd conns
CSCvg09316	Cisco Firepower Threat Defense Software Policy Bypass Vulnerability
CSCvg20782	Identified Vulnerabilities associated with the CVEs from Oracle MySQL Patch Updates
CSCvg25287	Add `mysql-server.err` file to logrotate.d in Firepower Threat Defense
CSCvg37391	Migrated access control policy deploy fails since it has FQDN objects
CSCvg42033	prune to cleanup unused data in eoattributes table at vms.db to reduce backup file size
CSCvg43389	ASA traceback due to 1550 block exhaustion.
CSCvg65072	Cisco ASA sw, FTD sw, and AnyConnect Secure Mobility Client SAML Auth Session Fixation Vulnerability
CSCvg73042	SSL Cache missing session info leading to `ERR_SSL_PROTOCOL_ERROR` in the browser for SSL websites
CSCvg84474	Space in port range for an access control policy rule causes error that prevents rule editing
CSCvg85765	ASA5506 traceback on policy deploy
CSCvg97808	Cisco Firepower System Software Transport Level Security Extensions Denial of Service Vulnerability
CSCvg99327	Cisco Firepower System Software Transport Level Security Denial of Service Vulnerability
CSCvh07446	On 7000/8000 devices, many IPs in a single access control rule will match rule incorrectly
CSCvh20742	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvh22181	Failures loading websites, such as mail sites, using TLS 1.3 with SSL inspection enabled

Caveat ID Number	Description
CSCvh46202	Slow 2048 byte block leak due to fragmented traffic over VPN
CSCvh48668	Device overrides not correctly applied to access control policy.
CSCvh53901	SFDataCorrelator cores when reading invalid fingerprint type from database
CSCvh68521	On 8000 series stack, with **Maint on sec fail** setting enabled, stack health is in compromised state
CSCvh77721	Standby SFDataCorrelator fails to connect to Sybase after Management Center pair establish/resume
CSCvh83145	ASA interface IP and subnet mask changes to `0.0.0.0 0.0.0.0` causing outage of services on interface
CSCvh84511	Cisco FireSIGHT System URL-based Access Control Policy Bypass Vulnerability
CSCvh85246	ssl inspection can be limited by a **Do-Not-Decrypt** rule specifying one or more common names
CSCvh85580	`ids_event_alerter` core when processing connection events
CSCvh89095	Firepower Management Center allows deleting Interface Object being used in SLA monitor object
CSCvh90092	AQ task selection ignores few groups when large no of groups present causing 8 hr delays in deploy
CSCvh95600	Need consistent identifier for lines of ssl debug log output
CSCvh95807	SSL FLow Errors reported when accessing ECDSA signed websites
CSCvh97594	ssl inspection cache can become unbalanced, leading to premature removal of recently used items
CSCvi09305	Some SSL connections slow or fail under a **Do-Not-Decrypt** SSL policy action
CSCvi12354	Threat Defense member in intra-cluster environment is not able to be re-added in Management Center
CSCvi16029	Cisco Adaptive Security Appliance WebVPN Denial of Service Vulnerability
CSCvi29845	Cisco Firepower detection engine memory leak vulnerability
CSCvi58865	SSL policy with URL category rules specifying decryption can cause browser errors
CSCvi63888	SSL errors might occur when resumed sessions are not decrypted
CSCvi66905	PIM Auto-RP packets are dropped after cluster master switchover
CSCvi97721	The memcap for Security Intelligence URL feeds needs to be increased for devices 4GB total memory
CSCvj07038	Firepower devices need to trust Threat Grid certificate

Caveat ID Number	Description
CSCvj45594	SFDataCorrelator core when timing-out old host info on a slow Firepower Management Center
CSCvj48931	Firepower recommendation updates task never runs
CSCvj63196	Workaround for Sybase issue: After snort engine update, policy deployment fail abruptly

Issues Resolved in Version 6.2.0.5

The following table addresses resolved caveats at the time of publication of these release notes. If you have a Cisco support contract, use the following dynamic queries for an updated list of resolved caveats, run the provided query in the Bug Search Tool:

- Resolved Firepower Management Center caveats in Version 6.2.0.5
- Resolved Firepower Management Center Virtual caveats in Version 6.2.0.5
- Resolved ASAFirePOWER caveats in Version 9.7.x

Table 1: Security Issues in Version 6.2.0.5

Caveat ID Number	Description
CSCto19832	OpenLDAP needs to be upgraded or patched in ASA running Firepower Threat Defense process
CSCve26946	Cisco Firepower System Software Bit Torrent File Policy Bypass Vulnerability
CSCve91584	Cisco Firepower Management Console Security Intelligence Objects Denial of Service Vulnerability
CSCvg35384	snort crash "deleteSessionByKey" found when access control policy edited and malware traffic is sent
CSCvg35618	Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability
CSCvh79732	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh81737	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh81870	Cisco Adaptive Security Appliance Denial of Service Vulnerability

Caveat ID Number	Description
CSCto19051	Resolve any vulnerabilities in ASA/Firepower Threat Defense Heimdal code
CSCuy91788	ASAv: Free memory is reported as negative in an OOM condition

Caveat ID Number	Description
CSCuy96471	Firepower Threat Defense device runs out of memory when nearing 35 million open connections.
CSCuz68504	Dynamic Analysis Summary not showing full report
CSCva02655	ASA sends invalid interface id to SFR module for clientless VPN traffic
CSCva17189	References to "Adaptive Security Appliance" when booting Firepower Threat Defense
CSCva42408	Event Analysis UI: Domain column disappears after switching to secondary Firepower Management Center
CSCva97863	971 EST - Console hang on show capture
CSCva98532	Firepower Threat Defense inline is not blocking MPLS-switched TCP session it should block
CSCvb39082	Smart License: Cluster role change triggers authorization renewal.
CSCvb40875	Default inspection statements missing on ASA 5500-x and 2100 device running FirepowerThreat Defense
CSCvb50750	Cisco ASA failure during failover with SIP traffic.
CSCvb57936	Unable to save AD join credentials from Edit Realm page
CSCvb58087	Redundant service group objects are incorrectly removed from object-group searches.
CSCvb81438	TCP connections might fail through a Threat Defense cluster with inline mode interfaces
CSCvc21275	Internal error on editing the NAT policy after import
CSCvc24310	Correlation events showing up with random Security Intelligence Category.
CSCvc36805	Firepower Threat Defense IKEv2 NAT-T gets disabled after reboot
CSCvc38425	ASA with FirePOWER module generates traceback and reloads or causes process not running
CSCvc46502	Firepower Threat Defense Cluster 9K block depletion with fragmented traffic
CSCvc71764	Blade got stuck in slave bulk sync after changing the CCL
CSCvc82146	ASA traceback in threadname **Datapath**
CSCvc91839	Unable to deploy policy on Firepower Threat Defense devices due to wrong XML parsing
CSCvc92982	Unable to delete configured Auto NAT from Firepower Management Center
CSCvc94586	CTS traffic not propagating Firepower Threat Defense inline mode
CSCvc97734	Deployment fails when management-only enabled on port-channel interface

Caveat ID Number	Description
CSCvd03421	Number of interfaces on active and standby are not consistent.
CSCvd08709	Asymetric path ICMP traffic fails through distributed clustering
CSCvd10251	Insufficient TCP options validation at 2nd normalizer in **tcp_norm_parse_ts**
CSCvd20408	Threat Defense: Interface capture on lina CLI causes all traffic to be dropped on data-plane
CSCvd23471	ASA may traceback while loading a large context config during bootup
CSCvd26939	SNMP lists same Hostname for all Firepower Threat Defense managed devices
CSCvd33044	Firepower Threat Defense traceback while deploying access control policy
CSCvd34694	Enabling SSL Decryption blocks legitimate traffic
CSCvd41052	Scheduler Queue Corruption leads to connectivity failures or failover problems after 9.6(2)
CSCvd56292	Default "global_policy" service-policy removed after reboot
CSCvd75631	Firepower Threat Defense DHCP Client tries to request a DHCP address instead of declining
CSCvd78303	ARP functions fail after 213 days of uptime, drop with error **'punt-rate-limit-exceeded'**
CSCvd79863	Firepower Threat Defense OSPF with ECMP, packets sent to peer in down state for existing connections
CSCvd93621	Unable to edit performance settings in advanced section of access control policy
CSCvd97568	Firepower Threat Defense traceback observed during failover synchronization.
CSCve03387	Proxy ARP information for SSH NLP NAT not updating on Firepower Threat Defense Device upon failover
CSCve04326	Slave should have use CCL to forward traffic instead of blackholing when egress interface is down
CSCve13410	Upgrading the ASA results in no valid adjacency due to track configure on the route
CSCve23091	Auto-RP packet is dropped due to no-route - No route to host
CSCve25577	Interfaces on slaves in shutdown if Firepower Management Center deployment results in failure
CSCve34640	SSL policy causing inspection engine (Snort) processes stop unexpectedly
CSCve46883	Firepower Threat Defense Diagnostic Interface does Proxy ARP for br1 management subnet
CSCve63762	ASA-SM: Interface VLANs going to admin down after reload.

Caveat ID Number	Description
CSCve70416	SSL policy with decrypt-resign action does not decrypt traffic with ECDSA certificates
CSCve71661	Firepower Threat Defense - Multicast and BPDU traffic dropped due to dst-l2_lookup-fail
CSCve74524	User Agent does not properly report group names with special characters in the name
CSCve84791	Capturing asp-drop causes unexpected ASA failure
CSCve96463	False positives for TCP Session Hijacking in routed deployments
CSCve97395	Syslog and SNMP do not work for Prefilter Policy on Firepower Threat Defense
CSCve97874	ASA: Low free DMA Memory on Versions 9.6 and later (Applies to ASA 5515 ONLY)
CSCvf10088	Migration fails when access-list contains VXLAN port
CSCvf11695	Duplicate host entries in flow-export action cause traceback after policy deployment
CSCvf13106	EIGRP system defined template for every time deployment is not working
CSCvf22930	Firepower 9300 running ASA 9.7.1.10 Firepower Threat Defense high availability traceback in Datapath
CSCvf25415	Spaces in IP range in access control policy can cause deploy to fail
CSCvf26676	With SSL inspection, Snort can terminate unexpectedly in SideChannel
CSCvf34791	Install 6.2.2-1290 on an ASA with Firepower Services-- ASA fails unexpectedly.
CSCvf44801	Intrusion rule with multiple negations can be trigger false positives
CSCvf58260	Categories missing from Security Intelligence events
CSCvf64643	ERROR on Firepower Threat Defense device: **Captive-portal port not available. Try again**
CSCvf72930	Firepower Threat Defense may traceback in Thread Name **appAgent_monitor_nd_thread** during registration
CSCvf81222	Memory leak in 112 byte bin when packet hits PBR and connection is built
CSCvf90278	ASA/Firepower Threat Defense traceback when enabling or clearing the packet capture buffer
CSCvf96656	After creating an access control rule with app filters via REST API, cannot access policy from UI
CSCvg00356	BitTorrent traffic not detected when traffic path includes a proxy
CSCvg07052	RealID+TempID in Sybase makes **SFDataCorrelator** incorrectly assign TempID to new logins
CSCvg17478	Traceback with Show OSPF Database Commands

Caveat ID Number	Description
CSCvg22873	Threat Defense Virtual: Azure, **waagent.log** file grows without bounds and needs to rotate
CSCvg23945	ASA panic/crash **spin_lock_fair_mode_enqueue**: **Lock (mps_shash_bucket_t)** is held for a long time
CSCvg25358	Set oom-killer priorities
CSCvg25694	Crash on Standby Firepower 4140 module after Policy deployment.
CSCvg28189	Snort memory leak causing complete traffic outage and goes into D state
CSCvg34306	ENH - The memcap for Security Intelligence URL feeds needs to be increased.
CSCvg52995	Unable to save configuration in system context after enabling password encryption in ASA
CSCvg53208	Application protocol field missing in connection events
CSCvg54460	ASA FirePOWER module managed by ASDM, **ADI.conf** removed on policy deployment
CSCvg58941	Elevated CPU Using Flow-Offload & High Rate of Flow Table Collisions
CSCvg60217	AppId is sharing incorrect high availability pair information for unmonitored networks
CSCvg60323	D/R HTTPS connections fail in browsers that enforce OCSP must staple
CSCvg65044	When network packets are transmitted out-of-order, some SSL sessions may not be established
CSCvg66697	segfault in **ssl_handshake::sig_hash**
CSCvg66706	**SFDataCorrelator** deadlock core due to slow User Identity event processing
CSCvg66844	Excessive log messages "**found no record for Realm**" and excessive database queries
CSCvg71421	Archive Cache Pruning May Not Work
CSCvg76652	Default DLY value of port-channel sub interface mismatch
CSCvg90403	Blocks of size 80 leak observed when IRB is used in conjunction with multicast traffic
CSCvg96525	**SFDataCorrelator** deadlock during whitelist host evaluation
CSCvg97541	Firepower Threat Defense prefilter policy only fast-paths single direction of bidirectional flow
CSCvg97874	FireAMP Cloud events are not available for eStreamer clients
CSCvh12075	Firepower Threat Defense devices in high availability might go into reboot loop one after the other

Caveat ID Number	Description
CSCvh18106	Firepower Management Center- Flexconfig-Removal of EIGRP Authentication every time during deployment
CSCvh21873	**SFDataCorrelator** on Firepower Management Center repeatedly crashes for corrupt user login event
CSCvh81331	Add support for i) wild card port numbers in host cache ii) overwriting port service AppId
CSCvh91577	**IDSEventAlerter:config [ERROR] Unrecognized keyword: "ssl_policy_UUID"**

Issues Resolved in Version 6.2.0.4

The following table addresses resolved caveats at the time of publication of these release notes. If you have a Cisco support contract, use the following dynamic queries for an updated list of resolved caveats, run the provided query in the Bug Search Tool:

- Resolved Firepower Management Center caveats in Version 6.2.0.4
- Resolved Firepower Management Center Virtual caveats in Version 6.2.0.4
- Resolved ASA FirePOWER caveats in Version 9.7.x

Table 2: Security Issues in Version 6.2.0.4

Caveat ID Number	Description
CSCvc72421	Security Review for OpenSSH: CVE-2016-10009 , CVE-2016-10010 , CVE-2016-10011 , CVE-2016-10012
CSCvd97249	Cisco Firepower Detection Engine SSL Decryption Memory Consumption Denial of Service Vulnerability

Caveat ID Number	Description
CSCto19051	Resolve any vulnerabilities in ASA/Firepower Threat Defense Heimdal code
CSCuu97541	Turn off older SSL/TLS versions and ciphers
CSCuy36266	Autonegotiation automatically enabled after 5.4.x patch is applied
CSCuy91788	ASAv: Free memory is reported as negative in an OOM condition
CSCuy96471	Firepower Threat Defense: When nearing 35 million open connections, box runs out of memory
CSCuz44985	Erroneous syslog messages cause excessive upgrade times/failures
CSCva02655	ASA sends invalid interface id to SFR for clientless VPN traffic
CSCva17189	References to "Adaptive Security Appliance" when booting Firepower Threat Defense

Caveat ID Number	Description
CSCva97863	971 EST - Console hang on **show capture**
CSCva98532	Firepower Threat Defense inline is not blocking MPLS-switched TCP session it should block
CSCvb39082	SmartLic: Trigger auth renewal from the app for cluster role change
CSCvb40875	Default inspect statements are missing on ASA 5500-x and 2100 device running Threat Defense
CSCvb50750	Cisco ASA core during failover with sip traffic
CSCvb58087	Object-group-search redundant service group objects are incorrectly removed
CSCvb81438	TCP connections might fail through a Threat Defense cluster with inline mode interfaces
CSCvb81481	No Input/Output packet for Port-channel in Firepower Threat Defense 4100
CSCvc36805	Firepower Threat Defense IKEv2 NAT-T gets disabled after reboot
CSCvc37849	Cannot edit intrusion policy after upgrade to 6.1 due to undefined rule state
CSCvc38425	ASA with FirePOWER module generates traceback and reloads or causes process not running
CSCvc46502	Firepower Threat Defense Cluster 9K block depletion with fragmented Traffic
CSCvc82146	ASA traceback in threadname Datapath
CSCvc84721	Health monitor error: "**The cloud databases for these appliances are not synced**"
CSCvc91839	Unable to deploy policy on Firepower Threat Defense devices due to wrong XML parsing
CSCvc92397	Webpages loads very slowly when URL retry is enabled
CSCvc92982	Unable to delete Configured Auto NAT from FMC
CSCvc94586	CTS traffic not propagating Firepower Threat Defense Inline mode
CSCvc97734	Deployment fails when management-only enabled on port-channel interface
CSCvd03421	Number of interfaces on Active and Standby are not consistent.
CSCvd10251	Insufficient TCP options validation at 2nd normalizer in **tcp_norm_parse_ts**
CSCvd23471	ASA may traceback while loading a large context config during bootup
CSCvd26939	SNMP lists same Hostname for all Firepower Threat Defense managed devices
CSCvd33044	Firepower Threat Defense traceback at **"cli_xmlserver_thread"** while deploying access-control policy

Caveat ID Number	Description
CSCvd41052	Scheduler Queue Corruption leads to connectivity failures or failover problems after 9.6(2)
CSCvd51463	Custom detection/Clean list is incorrect with multiple file polices in use
CSCvd56292	Default "global_policy" service-policy removed after reboot
CSCvd75631	Firepower Threat Defense DHCP Client tries to request a DHCP address instead of declining
CSCvd78303	ARP functions fail after 213 days of uptime, drop with error '**punt-rate-limit-exceeded**'
CSCvd79863	Firepower Threat Defense OSPF with ECMP, packets sent to peer in down state for existing connections
CSCvd82225	Queries against temp merge tables may fail
CSCvd97568	Firepower Threat Defense traceback observed during failover synchronization.
CSCve03387	Proxy ARP information for SSH NLP NAT not updating on Firepower Threat Defense Device upon failover
CSCve04326	Slave should have use CCL to forward traffic instead of blackholing when egress interface is down
CSCve08525	URL DB Download Fail with error -8
CSCve10708	Upgrade file-transfer from Firepower Management Center to Firepower device times out after one hour
CSCve13410	Upgrading the ASA results in No Valid adjacency due to track configure on the route
CSCve23091	Auto-RP packet is dropped due to no-route - No route to host
CSCve25577	Interfaces on SLAVES in shutdown if Firepower Management Center deployment results in failure
CSCve28417	[NSS] Snort 6 Core - AAB - in SnortPcre of file **detection_options.c**
CSCve34640	SSL policy causing inspection engine (snort) processes stop unexpectedly
CSCve46883	Firepower Threat Defense Diagnostic Interface does Proxy ARP for br1 management subnet
CSCve55696	UIMP continues to attempt import for deleted users
CSCve58157	Host Input Daemon exits when interface is IPv6 (no IPv4)
CSCve58826	Issues with multiple pending **UserEnforcementSnapshot** tasks
CSCve63762	ASASM: Interface vlans going to admin down after reload.
CSCve64913	Database Limits are not correct for Firepower Management Centers (2500, 4500)

Caveat ID Number	Description
CSCve71661	Firepower Threat Defense - Multicast and BPDU traffic dropped due to **dst-l2_lookup-fail**
CSCve82410	Port Scan doesn't block scans
CSCve85240	Access control policy uneditable if copying large Policy, insert/move 50+ rules into category
CSCve85996	Deployment timeouts after 30 minutes due to expand of ACE during deployment
CSCve86182	Reserved Characters in AC/ Prefilter policy rule names may fail Firepower Threat Defense Deployments
CSCve88096	File Events may incorrectly show **"Device Not Activated"** for capacity handled files
CSCve94530	**SFDataCorrelator** signal-6 core on Firepower Management Center after reconfigure
CSCve97874	ASA: Low free DMA Memory on versions 9.6 and later
CSCve97997	Multiple CLAM update tasks created in the AQ ,during device registration.
CSCvf02972	Inspection engine (snort) can stop unexpectedly during an SSL rule update
CSCvf11695	Duplicate host entries in flow-export action cause traceback after policy deployment
CSCvf12124	Third Party Vulnerability Maps won't save
CSCvf14953	Health Alert for CPU usage on cores dedicated to Radware DefensePro service
CSCvf22930	FP9300 9.7.1.10 Threat Defense high availability traceback in Datapath
CSCvf23425	SSL handshake error and timeout occurs when HTTPS traffic is passed through GRE tunnel
CSCvf29140	Avoid deleting latest version for **bcdb_rep*.bin** file
CSCvf34791	Install 6.2.2-1290 on an ASA with Firepower Services- ASA fails unexpectedly
CSCvf41773	Threshold configuration files have old unneeded policies
CSCvf50819	**AS Path prepend** command truncated while deployed
CSCvf52889	Delay of end of connection events for SSL traffic
CSCvf54853	Large database size for devices upgraded from 6.1.0.x to 6.2.0.x
CSCvf54986	Policy import from SFO or deleting realms fails with unreachable directory servers
CSCvf55219	Heap out of bounds read in **DecodeCiscoMeta()**
CSCvf55850	access-list rules missing after policy deployment on Firepower Threat Defense
CSCvf56267	Duplicate email addresses causes Firepower Management Center processes to fail

Caveat ID Number	Description
CSCvf59214	User sessions without email might cause database issues
CSCvf59399	Memory growth in **SFDataCorrelator** due to User Identity
CSCvf62276	Missing IP address in AMP cloud malware events
CSCvf63022	Application isn't being identified for RTP stream
CSCvf63871	Inspection engine CPU usage high if SSL policy or captive portal are enabled
CSCvf64643	ERROR on Firepower Threat Defense device: **Captive-portal port not available. Try again**
CSCvf67573	Errors during interface creation/deletion and config save
CSCvf69012	Unassigning Flexconfig object that has MPF config removes service-policy and pmap but not class-map
CSCvf70092	Resource Leak in **SFTop10Cacher** leads to deadlock
CSCvf72930	Firepower Threat Defense may traceback in Thread Name **appAgent_monitor_nd_thread** during registration
CSCvf74790	**OGS** and **TCM** commands are negated by Firepower Management Center during policy deployment
CSCvf76566	S4000-K9 // Cannot add object to the network group (FMC 682412623)
CSCvf77469	Packet loss during **Server Hello** when SSL policy verdict is **Do Not Decrypt** causes failures
CSCvf77493	Management interfaces are missing on Firepower Management Center 4500, 2500, or 1000
CSCvf78924	Maximum Transmission Unit (MTU) setting ignored on managed devices, leading to dropped packets
CSCvf80717	TCP SACK in conjunction with SSL decryption can cause connections to stuck
CSCvf81222	Memory leak in 112 byte bin when packet hits PBR and connection is built
CSCvf86080	**SFDataCorrelator** needs to log incorrect timestamp on bucketized partitioned tables
CSCvf86435	If Drop threshold is configured in Intelligent Application Bypass, all traffic will be trusted
CSCvf86487	Intelligent Application Bypass drop percentage does not work as expected
CSCvf87538	Syslog ID is reset to '111111' when editing syslog settings
CSCvf89183	Large Deploy Bundles and slow links causes deploy to fail
CSCvf90278	ASA/Firepower Threat Defense crashes when clearing the packet capture buffer

Caveat ID Number	Description
CSCvf92782	PAT pool fails to be enabled on Japanese GUI
CSCvf95108	**Action_queue** tables not pruning successful/failure tasks
CSCvf95494	Routes are not applied on a 7000/8000 series devices in Cluster
CSCvf97107	Retransmit delay when first packet lost with decrypt - resign or do not decrypt SSL policy action
CSCvg08745	Snort segfaults and coring while processing FTP traffic.
CSCvg08988	Access Control Rule is not created in snort if source zone and destination zone are the same
CSCvg17478	Traceback with Show OSPF Database Commands
CSCvg23945	ASA panic/crash **spin_lock_fair_mode_enqueue**: **Lock (mps_shash_bucket_t)** is held for a long time
CSCvg25694	Assert Traceback, thread name : **cli_xml_server**
CSCvg32885	Unable to edit or Deployment missing some of the access control rules after upgraded to 6.2.0.3
CSCvg36672	Need a way to prioritize user driven deployment tasks in Action Queue
CSCvg42347	6.2.0.3 upgrade failed on standby 4140 at script **800_post/755_reapply_sensor_policy.pl**
CSCvg52995	Unable to save configuration in system context after enabling password encryption in ASA
CSCvg56681	Upgrade framework scripts incorrectly delete rc symlinks
CSCvg58941	Elevated CPU Using Flow-Offload & High Rate of Flow Table Collisions
CSCvg72583	Archive Cache Loading Could be in Deadlock
CSCvh12075	Firepower Threat Defense devices in high availability might go into reboot loop one after the other

Issues Resolved in Version 6.2.0.3

The following table addresses resolved caveats at the time of publication of these release notes. If you have a Cisco support contract, use the following dynamic queries for an updated list of resolved caveats, run the provided query in the Bug Search Tool:

- Resolved Firepower Management Center caveats in Version 6.2.0.3
- Resolved Firepower Management Center caveats in Version 6.2.0.3
- Resolved ASA FirePOWER Module caveats in ASA Version 9.7.x

Table 3: Security Issues in Version 6.2.0.3

Security Issue CSCve02069	2048 byte block depletion with continuous SSL traffic and decrypt resign enabled on Threat Defense
Security Issue CSCvd07072	Cisco Firepower SSL Logging Denial of Service Vulnerability
Security Issue CSCve12652	Cisco Firepower System Software Secure Sockets Layer Policy Bypass Vulnerability

Caveat ID Number	Description
CSCuy65203	Inline result showing **would have dropped**
CSCva30652	spurious high unmanaged disk usage on `/dev/shm` alerts
CSCvb22670	SFDCNotificationd dumps core if stopped after SFDataCorrelator
CSCvb34534	access control policy search highlight incorrectly highlights
CSCvb44254	ASA 5506-X Firepower Threat Defense Reset Button
CSCvb72561	Mperf causing high CPU and stays constantly high .
CSCvb87476	Proxy configuration can't be saved from UI, under some circumstances
CSCvc06133	Firepower Management Center freezes when attempt is made to sort the App Detectors
CSCvc06397	Upgrade ASA on Firepower Threat Defense managed by Management Center breaks Malware cloud lookup
CSCvc09017	Show Nat flows on Firepower 7000/8000 series devices displays incorrect data
CSCvc39550	Unable to expand or scroll if more than 11 DHCP relay agents configured in Management Center
CSCvc46599	Error message **Unable to translate SSL cipher suite 65535** needs cleaning up
CSCvc46914	Rule copy and paste reset to top instead of the rule being edited
CSCvc49556	Diskmanager not managing `/var/cisco/umpd` properly
CSCvc51553	Unclear to user that DB check is running after ungraceful shutdown
CSCvc54659	Sub-interface entries not getting removed from bridge group interface after net-mode change
CSCvc57886	**Search** in access control policy returning incorrect results.
CSCvc59913	Mismatched VLAN tagged traffic has inconsistent access control rule matches.
CSCvc66770	Mishandled rule index numbers on multipage access control policies with collapsed rule categories

Caveat ID Number	Description
CSCvc68564	logrotate fails if permission on .conf file is incorrect - perm should be checked
CSCvc91394	Making minor changes to included/excluded users in a realm may cause unexpected behavior
CSCvc94207	Use of **manage_procs.pl** can result in a stack coming out of maintenance mode
CSCvc94589	Evaluation of sfims for OpenSSL Jan 2017
CSCvc96254	Route cannot be added under Management Interface
CSCvc96927	Management Interfaces Proxy settings disabled after 6.1.0 Management Center upgrade
CSCvc99959	Possible error in PDF/SWF decompression
CSCvd01405	Health monitoring for 8000 series firmware needs to try again for comms failure
CSCvd15607	DHCP server : Not able to configure DHCP server on BVI member (Redundant) - Transparent mode.
CSCvd16631	Excessive logging from sip preprocessor function SipSessionSnortCallback
CSCvd22778	Firepower Threat Defense high availability creation failed due to DB lock issue
CSCvd27999	`PerlMessageHand_11` core on Firepower Management Center Virtual while system is shutting down
CSCvd28945	modbus false postive on **MODBUS_BAD_LENGTH**
CSCvd35905	upgraded 6.x Management Center incorrectly deploys obsoleted detectors to 6.x devices
CSCvd37120	Snort is unable to map the filename if there are unsupported characters.
CSCvd39490	ADI discards all but one IP address from a session notification
CSCvd51190	Snort reloads cause memory leaks and CPU increase
CSCvd51302	When import HTTPS Server Certificate fails, UI is blank without error
CSCvd56035	Custom NAP rule with inline normalization enabled does not enable normalization
CSCvd59199	Mismatch between internal database entries prevents correct session propagation
CSCvd62879	Repeated same DiskMgr logs flooding messages log - causing small log retention period
CSCvd70549	Query Cisco CSI for Unknown URLs option is not properly synchronized in Management Center pairs
CSCvd73687	Access Control Policy page conflict detection can show conflicts when there are none.
CSCvd78338	Correlation Events and Syslog Events show incorrect local rule SID
CSCvd86594	Need ability to enable PPTP inspection

Caveat ID Number	Description
CSCvd89890	Policy deploy hangs at 40% with the object names end with [_]
CSCvd91019	Unable to delete third party vulnerabilities when the host count associated with them is > 100
CSCvd94044	7000 and 8000 Series Device with Passive Interface does not Failover when Active device powers off
CSCvd95667	Data channel traffic on windows FTP server aren't matching the pin hole session as expected
CSCvd96322	CSM backup failed on Secondary Firepower Management Center
CSCvd99119	Unable to import if Access Control rules has Realm as matching condition
CSCvd99574	Snort process at 100% and takes excessive amount of time to parse IPS rules.
CSCve02220	eStreamer certificate generates errors with a McAfee ESM generationQualifier verification failed
CSCve08217	**Maximum File Events** limit reduces to smaller number after upgrade to 6.1.0
CSCve08961	Stack entering bypass due to disk space health alert
CSCve10406	SFDataCorrelator will not stop on Threat Defense device due to database connection corruption
CSCve10708	Upgrade file-transfer from Firepower Management Center to Firepower device times out after one hour
CSCve11915	POP3 payload inspection not proper on snort with the file detection policy
CSCve15155	Host input operations can overwhelm high availability transactions
CSCve17116	Access control rule is not matched correctly if src zone and dst zone have different types
CSCve18975	Nothing is shown when clicked on **Policy Assignements**
CSCve34181	Static URL/DNS lists are not included in backup
CSCve34924	When expanding individual categories in Access Control Policy rule ID changes
CSCve35722	Running Patch Uninstaller causes **cc-integrity.sh** to fail; no UI.
CSCve35816	SFDataCorrelator segfault due to null pointer dereference in **handle_host_address_changes()**
CSCve39775	Multiple login messages different username and same realm/IP/timestamp scrambles SFDaco
CSCve41306	Firepower Management Center **Interface Type Mismatch with Syslog Server Ip Type** error

Caveat ID Number	Description
CSCve44987	eStreamer service sends corrupt messages and spams log files with **Not connected**
CSCve46036	SFDataCorrelator segfault due to null field in internally generated logoff event
CSCve46186	Snort memcals for startup memory incorrect on Firepower Threat Defense
CSCve47333	Management Center not deactivating smart licenses for Firepower Threat Defense devices
CSCve47800	Port Scan: IP Protocol scanning not getting detected.
CSCve47868	Snort not triggering Event 123:7 `FRAG3_ANOMALY_BADSIZE_LG`
CSCve47923	eStreamer log spam **Unable to open directory**
CSCve51315	**record_count** for interface stats from the sensor are being set to 0, coring SFDatacorrelator.
CSCve53544	Firepower Management Center high availability sync fails if file name contains 2 dots [**..**]
CSCve61591	BitTorrent traffic not blocked consistently on resumed sessions.
CSCve63017	Migration lock not removed even if migration fails
CSCve64643	REST API internal error when removing AP rule from API that moved via GUI
CSCve72760	Missing column netmap_num from the join on event_extra_data table.
CSCve73229	Platform settings applied to more than 1 Threat Defense device do not vary
CSCve73601	Threat Defense: Blocking Facebook post/chat/comments/likes application not working for Firefox
CSCve74585	SFDataCorrelator crash or exit when event table **contains large highest index**
CSCve74902	REST identity application and ADI leak File Descriptors
CSCve79949	Poor performance of packet logs UI due to query not using index
CSCve82386	Configuring an IP pool for a diagnostic port channel interface on an Threat Defense cluster fails
CSCve85240	Access control policy uneditable if copying large Policy, insert/move 50+ rules into category
CSCve90940	DNS Security Intelligence feeds are not automatically push to sensors
CSCve94250	SFDataCorrelator coring due to ids_event_msg_map message being null
CSCve94848	MC2000 and MC4000 can rarely hang during boot
CSCve95026	**ids_event_alerter** causes high CPU on Threat Defense device when UUID is missing from EOAttributes

Caveat ID Number	Description
CSCve95168	Unicode file support over SMB on Firepwer Threat Defense
CSCve97997	Multiple CLAM update tasks created in the AQ ,during device registration.
CSCve99153	Access control policy/Pre-filter rules are negated and readded on usage of icmp objects
CSCve99203	256 low block count leads to traffic failures due to alloc to inspect snort
CSCve99622	Intrusion event of old session is missing after update and config deploy
CSCvf02208	Management Center: Deleting 1 category in nested access control policy deletes all categories
CSCvf05977	Firepower Threat Defense management interface link flaps when IPv6 gateway is configured
CSCvf09887	Performance graphs are inconsistent when **processed_total_packets** is 0
CSCvf09949	Incorrect access control rule is matched in Threat Defense device when it is setup in passive mode
CSCvf10781	SFDataCorrelator segfaults repeatedly when processing SSL certificate details
CSCvf15216	When SSL rules are enabled and sensor is over subscribed, rules are not correctly enforced.
CSCvf15265	SFDataCorrelator takes a long time to start due to large **firewall_rule_cache** table
CSCvf16288	after captive portal authentication, packet is incorrectly associated with realm ID 0
CSCvf16799	DH Ephemeral Keys with Known Key SSL Policy and session reuse causes client to close session.
CSCvf18368	Long traffic connections matching D**o Not Decrypt SSL** rules may be blocked
CSCvf22098	Management interface bootstrap fails with IPv6 only configuratiom and no available DHCPv4 servers
CSCvf36025	SFDataCorrelator segfaults during loading of compliance rules
CSCvf38056	SSL flows failing due to Flow tables and Flow ID's overflowing
CSCvf38081	SSL policy Category lookup fails for URLs that aren't in local database
CSCvf39476	Rules getting pushed after the **Default Block All Rule** on Firepower Threat Defense device
CSCvf43107	Estreamer Cores - SSLCert length handling
CSCvf54853	Large database size for devices upgraded from 6.1.0.x to 6.2.0.x
CSCvf55850	access-list rules missing after policy deployment on Firepower Threat Defense
CSCvf71086	Port-channel cannot be configured as a passive interface

Caveat ID Number	Description
CSCvf75781	Firepower Threat Defense device may leave cluster due to disk space alert

Issues Resolved in Version 6.2.0.2

The following table addresses resolved caveats at the time of publication of these release notes. If you have a Cisco support contract, use the following dynamic queries for an updated list of resolved caveats, run the provided query in the Bug Search Tool:

- Resolved Firepower Management Center Virtual caveats in Version 6.2.0.2
- Resolved Firepower Management Center Virtual caveats in Version 6.2.0.2
- Resolved ASA FirePOWER Module caveats in ASA Version 9.7.x

Caveat ID Number	Description
CSCvc57886	'Search' in access control policy returning incorrect results.
CSCva78299	access control Policy Report Differs from access control Policy Web Interface
CSCvc24013	Firepower Management Center not providing options to restrict ICMP types for certain codes
CSCvd69506	Network range with a space after the dash removes current and subsequent ACP rules
CSCvc10913	SFDataCorrelator polling for status of file analysis can fail in certain circumstances
CSCvd05788	Communication channel is blocked if recurring backup fails due to disk space on remote server
CSCvc09017	Show Nat flows on series 3 displays incorrect data
CSCvd14261	Fail to create Threat Defense high availability due to previous failed attempt
CSCve17179	Firepower Management Center high availability Sync can delete csm config files
CSCvd38500	Performance issue with Device listing page
CSCvd75631	Threat Defense DHCP Client tries to request a DHCP address instead of declining
CSCve47923	eStreamer log spam "Unable to open directory"
CSCve44987	eStreamer service sends corrupt messages and spams log files with "Not connected"
CSCuy50039	In Task Status page the task is stucked/spinning
CSCvd23471	ASA may traceback while loading a large context config during bootup
CSCvd04066	PBR config is blocked in FlexConfig
CSCvc53358	Interfaces not interpreted in hardware when contexts have 'lag' in their name

Caveat ID Number	Description
CSCvd37902	nse interface intialization has not occurred, but still receiving packets
CSCvc37876	Policy deploy fails due to inconsistency in HA Primary Threat Defense device in the backend
CSCvc56921	Altering logging settings like disabling syslog causes IPS and File policies to become disabled
CSCvc50598	Comparison reports for intrusion policy between 2 revisions is not working correctly
CSCvc04546	Discard does not rollback the updated Firepower Recommendation.
CSCvd60359	During backup intrusion policy error message on save should be intuitive.
CSCuy93365	Flowbit auto-resolution not working properly
CSCvd72697	Intrusion policy commit is slow because prepare statement is called multiple times
CSCva90055	change impact_flag on IPS/snort rule to red/orange/yellow/blue/gray
CSCvb28212	False warnings in DB Integrity Check for rule_comments/rule_comment_map
CSCvd32767	Unable to use objects inside IPS rules
CSCvc16184	Cannot re-arrange order of Network Analysis Rules
CSCvd62553	Policy deploy with NAP fails when adaptive profiles or auto detect setting is disabled in NAP
CSCvc48768	Search Option does not work for network objects under NAP editor
CSCur46880	Encapsulated traffic not matching hardware rules
CSCvd12448	Message "CSR access problem for ME 25" flooding dmesg
CSCvb40875	Default inspect statements are missing on ASA 5500-x and 2100 device running Threat Defense
CSCvd34691	Firepower: With SafeSearch on, users can't access multiple websites.
CSCvd55859	Snort segfault while processing malware cache.
CSCvd01332	With Safesearch configured but disabled, can lead to cores
CSCvd80218	Able to create Bridge group interface from global domain but device is in leaf domain
CSCvd90766	Deployment failed and internal error occurred when deleting Port channel inline set and deploy
CSCvd38316	Deployment is getting failed in high availability pair due to cluster inline-set interface.
CSCve01438	IP Address/Mask validation for Stanby Address missing during high availability formation

Caveat ID Number	Description
CSCvd83682	PPPoE User Name field should allow more characters
CSCve41306	Firepower Management Center 'Interface Type Mismatch with Syslog Server Ip Type' error
CSCvc10668	Unable to edit network objects when they are shared between devices
CSCvd65669	Standard ACL elements deployed in wrong order
CSCvb63720	Pseudo rule IDs are not unique when multiple DNS policies are deployed simultaneously
CSCvd09003	Checking for conflicts in variable sets doesn't work on network groups
CSCva92910	Too many addresses in HOME_NET results in failed deployment
CSCvd35243	C-groups modification during policy apply causes AAB to trigger.
CSCvb13791	Not able to login to Firepower 4100 using 'connect ftd' CLI
CSCvc94908	Qos Rule and interface widget doesn't display stats for QoS rules
CSCvd56292	Default "global_policy" service-policy removed after reboot
CSCvd18507	SFDataCorrelator segfault due to multi-threaded curl on HTTPS
CSCvb24824	Suspected latency during shared memory lookup (with URL Retry enabled)
CSCvc17167	URL Filtering stopped working due to major version change in the BC database
CSCvc92397	Webpages loads very slowly when URL retry is enabled
CSCvd90101	Report generation fails if the remote storage device is unmounted by another action
CSCvb16465	Security Intelligence category goes missing from Security Intelligence events after time
CSCve35816	SFDataCorrelator segfault due to null pointer dereference in handle_host_address_changes()
CSCvd76935	Unchecked host count growth after SFDataCorrelator reconfigure
CSCvd41052	Scheduler Queue Corruption leads to connectivity failures or failover problems after 9.6(2)
CSCvd74162	snort core in alert action.
CSCvd66343	Unable to block bittorent traffic when download is resumed after moving to a new network
CSCvc84361	Cisco Firepower Threat Defense and Cisco ASA with FirePOWER Module Denial of Service Vulnerability
CSCvc51173	Enabling SSL Policy may result in detection engine exits

Caveat ID Number	Description
CSCve02069	2048 byte block depletion with continuous SSL traffic and decrypt resign enabled on Threat Defense.
CSCvd93722	SSL Block action when Extended Master Secret is used with SSL Policy Known Key Decrypt
CSCvd41054	SSL Trusted CAs not deployed to sensor in some cases
CSCvc07857	Unable to disable Proxy Auth on Management Center by un-checking the proxy auth box
CSCvd11997	Database settings for a fresh deployment were not saved
CSCvd92322	ICMP Any in dst/src ports are saved incorrectly, which can result in broken pre-filter policy
CSCuy17170	After upgrading to 6.0, you cannot remove tasks from the taskbar
CSCvd04922	captive portal ntlm needs to handle token received in POST in addition to GET.
CSCvc93679	Firepower doesn't support userPrincipalName attribute for login with ISE / Active authentication
CSCvd94183	Intermittent failure in User Group lookup.
CSCvd77847	Management Center deployment fails due to error after creating a domain with devices
CSCva06227	Only 1500 Group Members are downloaded per group for an AD Realm
CSCvd45766	PxGrid sent MAB and internal ISE DB info to /var/log/messages cause outage on Management Center
CSCvd73834	Show user information in connection events for flows hitting early deny
CSCvd27278	UIMP fails importing all users if any user in the import list has been deleted
CSCvd71808	Users are removed from groups after scheduled user/group download
CSCva98254	Trying to delete an identity realm that is in use breaks the identity realm
CSCvc91320	"Failed to set user name for lights-out management" error when trying to change admin pw on FMC1500

Issues Resolved in Version 6.2.0.1

The following table addresses resolved caveats at the time of publication of these release notes. If you have a Cisco support contract, use the following dynamic queries for an updated list of resolved caveats, run the provided query in the Bug Search Tool:

- Resolved Firepower Management Center caveats in Version 6.2.0.1
- Resolved Firepower Management Center Virtual caveats in Version 6.2.0.1

- Resolved ASA FirePOWER Module caveats in ASA Version 9.7.x

Caveat ID Number	Description
CSCvb39435	Import of Access control Policy fails after upgrade to 6.1
CSCuz46366	Files not Sandboxed even when they are under file limit.
CSCvb69285	Policy Export fails partially in Firepower ASDM 6.1
CSCvb63352	SafeSearch breaks for retransmitted packets
CSCvb19716	FR Scale: Large File Copy (>4GB) Fails In SFTunnel
CSCvb82371	AC policy:Deployment failure is happening due to rule update issue
CSCvb08840	Policy cant be applied when SRU and automated deploys run in parallel
CSCvb63664	Passive Authentication with User Agent is not working for some users
CSCvb85231	Intrusion Email Alert is not working
CSCvb67792	Intrusion Emails no longer send after upgrading to 6.1
CSCvb24807	After 6.1 upgrade, stale entries in fireamp_cloud table cause UI problem
CSCvc51117	ASA to FTD migration may fail when invalid characters are used in an access-list name
CSCvb66611	ASA to FTD migration script creates nested port group objects, which causes deployment to fail
CSCvc09761	Cannot delete multiple rules at a time from ASA migrated Prefilter Policies
CSCvc52158	FQDN objects getting imported in FMC from migration tool generated .sfo
CSCvc36047	Having "0" at the object service PING service icmp echo 0 causes migration to fail
CSCvc46502	FTD Cluster 9K block depletion with fragmented Traffic
CSCvc48702	Migration fails when SLA monitor configuration is present
CSCvb20859	Migration report succeed but sfo creation & cleanup fails intermittently
CSCvc18928	Unable to import ASA config file in migration tool i.e 6.1.0-330
CSCva59135	When a migration activity in progress new migration need to be blocked
CSCuz90632	Backup done remotely can't be restored locally
CSCvb24755	Cardmanager on ASA5585-SSP-40 SFR exits due to a SIGPIPE signal
CSCuz40408	system support capture traffic parser rejects slash used in net filter
CSCvc54134	Device goes into reboot loop one after another until failover cable is removed

Caveat ID Number	Description
CSCvd20947	Unable to deploy AC policy to an FTD HA pair due to an object description with the '&' character
CSCvc33995	Context Explorer performance issues due to query incorrectly joining two event tables
CSCvb24378	Add ability to enable or disable default inspect configuration
CSCvb51382	FTD:Not able to login to converged cli using SSH
CSCvb52751	DB error after trying to add and survey network in whitelist profile
CSCvb27494	Cisco Firepower Malware Detection Bypass Vulnerability
CSCvc12727	snort core file when processing bltd packets
CSCvb67848	SSL widgets lack data labels in 6.1
CSCvb52344	some perl processes leak semaphores
CSCvc76394	Time-ordered EQE queries against partitioned event tables are not optimized
CSCvc05376	FMC Database issues causing Missing Passive User Sessions via User Agent failure
CSCvc49789	OptimizeTables.pl always fails on 6.1.0
CSCvb35499	Upgrade 6.0.1.2 to 6.1.0-330 fails at 560_install_version_masked_apps.pl
CSCvb01821	Policy deployment failing on FMC for VMWare
CSCvb96776	Frangelico: FMC HA: HA establishment fails due to large database files copy
CSCuz95008	eStreamer 5.4 clients are unable to process userID info on 6.0 Firepower Management Center metadata
CSCvc53293	Estreamer cores found in DC-HA setup
CSCvc30591	estreamer should use correct datastore for user identity mapping.
CSCvb88976	High unmanaged disk usage due to large flow_chunk table
CSCvc05323	snort is restarting and filling the disk with logs.
CSCvb79079	Adding syslog to Access Control Rule may result in loss of Real Time Eventing
CSCvb70786	ids_event_alert coring on 6.1.0
CSCvc44292	ids_event_alerter can crash or infinite-loop
CSCva23034	Latency in FMC HA synchronization
CSCvc10655	access control Policy Deployment failed after patch installation(6.1.0.330 to 6.1.0.1.30)
CSCvb91730	Attempting to change copper SFP interfeace type (inline/switched/routed) results in error

Caveat ID Number	Description
CSCva12703	SCALE: Health alarms are not displayed in UMS
CSCvc37927	Import fails with duplicate object name when the object names differs by case only
CSCvc52214	Import with config involving inline values fails
CSCvb02417	adaptive profiling performance scales badly in some cases
CSCvb42559	Firepower Management Center Smart Licensing bypasses Proxy Configuration when in eval mode
CSCvc06397	Upgrade on Off-box ASA-FTD breaks Malware cloud lookup.
CSCvc48851	Network Object not listed under the custom rule editor in NAP
CSCvc01694	Enable flow control on stacking interfaces
CSCvb78786	Network Discovery fails to parse zones in ND rules under certain conditions
CSCvb36847	Event QoS in legacy mode does not have an entry for interface stats
CSCva07265	Incorrect rule being logged for application rules that go pending.
CSCvb65052	Network based AC rules don't always match if preceded by a rule with application/url
CSCvb52057	SafeSearch dropping legitimate traffic since paf not marking packet flags
CSCvb46555	Segmentation fault at HttpPacketModification, httpModProcess
CSCvc49641	Snort process segfaults processing traffic in firewall (ngfw).
CSCvb77099	Traffic misses matching AC rule
CSCvc44398	URL not extracted from reassembled requests
CSCvb24768	Security Zone is "Unknown" after upgrade to 6.1
CSCvb55593	DHCP Relay configuration does not display in UI after 6.1 upgrade
CSCvb53091	platform settings page fails to load when applied to multiple stacks
CSCvb75591	Security Intelligence DNS Feed based logs not sent to external Syslog
CSCvb68226	Constant failovers on ASA high availability pair due to SSP module failure
CSCvb85507	Evaluation of sfims for CVE-2016-5195 (DIRTY CoW)
CSCvb97742	FP or AMP 7000/8000 series sensor kernel deadlock on 6.1
CSCvc26880	oom condition leads to repeated RCU stall warnings
CSCvc50232	SFR upgrade to 6.1.0 causes erroneous HA failovers and/or traffic loss under load on 5585-40,60
CSCvb96160	CWE-200 - M4-FMC - TLS/SSL Birthday attacks on 64-bit block ciphers

Caveat ID Number	Description
CSCvc23451	Evaluation of sfims for NTP November 2016
CSCva90011	FR - CVE-2011-3389 -TLS/SSL is enabling BEAST attack
CSCvc64050	ASAConfig uses wrong interface IDs after module unit rejoins multi context ASA cluster
CSCvb81176	Bird fix for segfault needs to be ported to EC and FR
CSCva89342	Interfaces get deleted on SFR during Multi-context HA configuration sync
CSCvb66334	OOM keeps running, series3 units keep crashing, requiring reboot
CSCvb40343	PM generated commands can break dhcrelay if using more than 22 lifs
CSCvc73128	Reservation of core 0 for system processes in arc.conf is ignored by ARC.pm
CSCvb57747	Deploy during intrusion rule update install may cause all subsequent policy applies to fail
CSCvb68292	Httpmod preprocessor does not get disabled when safesearch rules are disabled
CSCvc57533	Policy Deployment may fail due to delta splitting logic fail
CSCvc11916	Removing special characters from UI in AC rule does not remove characters from lina config
CSCvb92968	Two PM instances running simultaneously
CSCva30652	spurious high unmanaged disk usage on /dev/shm alerts
CSCvc32479	Cannot load proxy information for dynamical analysis (sandbox)
CSCvb16413	URL Filtering option on GUI being unset/disabled intermittenly
CSCvb65642	Firepower FMC Risk Reporting has spelling mistakes!
CSCvb94393	SFDataCorrelator malware lookups take too long - UI shows timeout action
CSCuy91156	Cisco Firepower System Software FTP Malware Vulnerability
CSCvb40344	File policy oversubscription when many hosts process file.
CSCva89328	FTD gets into a bad state in which it has severe performance degradation
CSCuy65203	Inline result showing "would have dropped"
CSCvc08844	Retry packets never time out and keep being sent to Snort
CSCvc08057	Snort core is seen on FTD during rate limiting test
CSCvb74873	Snort crash during SMB inspection in file_capture_stop
CSCvb61018	some application and file policy combinations can cause snort to core

Caveat ID Number	Description
CSCvb52625	unexpected ACK packet for MDI malware file traffic connection
CSCvb62292	Cisco Firepower Detection Engine SSL Denial of Service Vulnerability
CSCvb92740	HTTPS pages take 30+ sec to load with SSL decryption and URL category rules enabled together
CSCvb38524	IPS and File detection is not working if Applications are FTP, FTP Data
CSCvc03589	Seg fault on SSL after policy apply
CSCvc11251	segfault in ns_net_mbrwq_release while processing SSL flow.
CSCvc55369	Snort segfault in process_ssl
CSCvc30521	SSL Handshake not completing for "Do Not Decrypt" action with large server certificate
CSCvb94411	SSL policy rules may match undecryptable actions too early in certain configurations
CSCvc09753	SSL rules with URL categories defined are not processed correctly
CSCvc10937	Platform settings policy so not appear to work for Firepower stacks
CSCvc43324	Changing admin user password may fail for systems not using LOM.
CSCux46182	"Failed to run troubleshoot script / failed (256)" on secondary DC.
CSCvc53628	'Available Ports' tab hangs when editing prefilter rule ports
CSCvb63264	Default Prefilter Policies are not imported properly on FMC2000
CSCvb03905	PrefilterPolicy DefaultAction Issue with 6.1.x FMC upgraded from 6.0.x managing 6.0.x FTD Device
CSCvc12080	Rules from prefilter policy do not retain order when saving policy
CSCvb46146	Don't allow different upgrade to start when upgrade is in failed state
CSCvc12702	bltd segfault processing checksum (computeChecksum).
CSCvb36748	captive portal support for ips on a stick
CSCuy05562	Deleting users from analysis->users doesn't remove sessions from sensor
CSCvc24316	Firepower Management Center does not handle Postured user session updates from ISE servers
CSCvb69906	Users are removed from groups after scheduled user/group download (database problem)
CSCvb92474	user_ip_map files being skipped while pushed from FMC to Sensor due to DaCo crash

Issues 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.
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.

Caveat ID Number	Description
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.
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.

Caveat ID Number	Description
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.
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.

Caveat ID Number	Description
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.
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.

Caveat ID Number	Description
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.
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**.

Caveat ID Number	Description
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.
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.

Caveat ID Number	Description
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.
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.

Caveat ID Number	Description
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.
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.

Caveat ID Number	Description
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.
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.

Caveat ID Number	Description
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.
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	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.