Resolved Issues in Version 6.2.2

The following table addresses defects resolved at the time of publication of these release notes. For an updated list of known issues, run the provided query in the Bug Search Tool.

If you have a Cisco support contract, use the Firepower Management Center query or the ASA FirePOWER module query as a dynamic search for all resolved bugs with a severity 3 and higher.

Table 1: Resolved Security Caveats in Version 6.2.2

Caveat ID Number	Description
Security Issue CSCve12652	Cisco Firepower System Software Secure Sockets Layer Policy Bypass Vulnerability

Table 2: Resolved Caveats in Version 6.2.2

Caveat ID Number	Description
CSCuu97541	turn off older SSL/TLS versions and ciphers
CSCux61528	Sensor managed by Management Center thinks it is managed locally
CSCuy08223	Firepower Management Center 6.0.0 User Interface does not show more than 8 User Agents
CSCuy17170	After upgrading to 6.0, you cannot remove tasks from the taskbar
CSCuy50039	In Task Status page the task is stuck/spinning
CSCuy65203	Inline result showing **would have dropped**
CSCva06227	Only 1500 Group Members are downloaded per group for an AD Realm
CSCvb00980	Detection engine, primary detection engine, alerting process health alert
CSCvb16465	Security Intelligence category goes missing from Security Intelligence events after time
CSCvb22670	SFDCNotificationd dumps core if stopped after SFDataCorrelator
CSCvb30960	Large flow introduces latency on all traffic in FirePower Service on ASA

Caveat ID Number	Description
CSCvb34534	access control policy search highlight incorrectly highlights
CSCvb44254	ASA 5506-X Firepower Threat Defense Reset Button
CSCvb57936	Unable to save AD join credentials from edit realm page
CSCvb71265	Firepower: Identity policy shows incorrect warning about Zones
CSCvb72561	Mperf causing high CPU and stays constantly high .
CSCvc06133	Firepower Management Center freezes when attempt is made to sort the App Detectors
CSCvc09167	Firewall rules may not be in sync with firmware rules following policy apply
CSCvc10913	SFDataCorrelator polling for status of file analysis can fail in certain circumstances
CSCvc33269	Document bug: Impact of Leap second on Firepower products
CSCvc37849	Cannot edit intrusion policy after upgrade to 6.1 due to undefined rule state
CSCvc46914	Rule copy and paste reset to top instead of the rule being edited
CSCvc59913	Mismatched VLAN tagged traffic has inconsistent access control rule matches.
CSCvc64185	Task getting created whenever Cloud Management option is selected
CSCvc66770	Mishandled rule index numbers on multipage access control policies with collapsed rule categories
CSCvc84721	Health monitor error: **The cloud databases for these appliances are not synced**
CSCvc90768	Excessive logging from sfbbhealthd process.
CSCvc91394	Making minor changes to included/excluded users in a realm may cause unexpected behavior
CSCvc95382	User identity lost due to limited identity timeout configuration
CSCvd04965	Performance issues related to High Availability
CSCvd11997	Database settings for a fresh deployment were not saved
CSCvd28945	modbus false postive on **MODBUS_BAD_LENGTH**
CSCvd29021	Cannot break Firepower Threat Defense high availability if one of the paired devices has failed
CSCvd35243	C-groups modification during policy apply causes AAB to trigger.
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.
CSCvd41054	SSL Trusted CAs not deployed to sensor in some cases

Caveat ID Number	Description
CSCvd51190	Snort reloads cause memory leaks and CPU increase
CSCvd51463	Custom detection/Clean list is incorrect with multiple file polices in use
CSCvd56035	Custom NAP rule with inline normalization enabled does not enable normalization
CSCvd57039	Deadlock in Firepower Management Center high availability syncronization
CSCvd59199	Mismatch between internal database entries prevents correct session propagation
CSCvd61965	micro engine failure failure with msg Microengine heartbeat stopped
CSCvd62536	apache not listening on loopback IPv4 when management interface has only ipv6 configured
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
CSCvd73834	Show user information in connection events for flows hitting early deny
CSCvd78338	Correlation Events and Syslog Events show incorrect local rule SID
CSCvd89890	Policy deploy hangs at 40% with the object names end with [_]
CSCvd90569	High availability Status health module should not run on device
CSCvd91019	Unable to delete third party vulnerabilities when the host count associated with them is > 100
CSCvd93722	SSL **Block** action when Extended Master Secret is used with SSL Policy **Known Key Decrypt**
CSCvd94044	7000 and 8000 Series Device with Passive Interface does not Failover when Active device powers off
CSCvd94183	Intermittent failure in User Group lookup.
CSCvd95667	Data channel traffic on windows FTP server aren't matching the pin hole session as expected
CSCvd97249	Firepower Threat Defense: block depletion with continuous SSL traffic and **decrypt resign** enabled.
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.
CSCve02069	2048 byte block depletion with continuous SSL traffic and **decrypt resign** enabled on Threat Defense

Caveat ID Number	Description
CSCve02220	eStreamer certificate generates errors with a McAfee ESM generationQualifier verification failed
CSCve04055	Docs have incorrect commands to suspend or resume Firepower Threat Defense high availability
CSCve08525	URL DB Download Fail with **error -8**
CSCve08961	Stack entering bypass due to disk space health alert
CSCve10406	SFDataCorrelator will not stop on Threat Defense device due to database connection corruption
CSCve11915	POP3 payload inspection not proper on snort with the file detection policy
CSCve13738	Check UUID of Firepower Management Center high availability pair and both having same UUID
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**
CSCve20634	Creating ngfw rules with [#] character prevent **event_alerter** from starting.
CSCve30147	Sub-domain SI objects cannot be deleted
CSCve32346	SIGABRT ActionQueueScrape cores in Firepower Management Center high availability
CSCve34090	snort stuck or signal 6 core with interactive block rule
CSCve34181	Static URL/DNS lists are not included in backup
CSCve34792	Threat Defense-NAT:Deployment fails when Auto nat group object values overlapped with interface IP.
CSCve34924	When expanding individual categories in Access Control Policy rule ID changes
CSCve35816	SFDataCorrelator segfault due to null pointer dereference in **handle_host_address_changes()**
CSCve37999	Deployment fails when SSL Platform Settings has deprecated RC4-SHA and RC4-MD5 algorithms configured
CSCve38488	after upgrade, sessions which were deleted were still present in sensor's firewall
CSCve39409	Cannot select **Inherit from base policy** check box
CSCve41306	Firepower Management Center **Interface Type Mismatch with Syslog Server Ip Type** error
CSCve41647	Sessions for local ISE users don't get deleted when delete is attempted

Caveat ID Number	Description
CSCve42702	Device Manager bootstrap aborted - URL category and reputations not populated in URL filtering rules
CSCve44987	eStreamer service sends corrupt messages and spams log files with **Not connected**
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.
CSCve51357	5506/5508/5516 Threat Defense console login does not work if console speed set to 115200 in rommon
CSCve53544	Firepower Management Center high availability sync fails if file name contains 2 dots [**..**]
CSCve53812	SFDataCorrelator still in local management mode after deployed from Management Center
CSCve54447	**iprep_proxy.conf** should encode special characters in pass for authetication
CSCve61591	BitTorrent traffic not blocked consistently on resumed sessions.
CSCve64643	REST API internal error when removing AP rule from API that moved via GUI
CSCve64763	eStreamer core when FireAMP event has no SHA
CSCve66196	Editing syslog server platform setting policy and deploy does not push the correct cli to device
CSCve71028	NTP Default Server addresses can be modified
CSCve72760	Missing column netmap_num from the join on **event_extra_data** table.
CSCve73110	Specific mysql statement causing 6.2.1 upgrade failure
CSCve73175	**RPC.conf** not getting properly re-enabled during resumed upgrades
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
CSCve81576	REST API : PUT - Multiple entries allowed for the same user in Access policy Rule
CSCve82386	Configuring an IP pool for a diagnostic port channel interface on an Threat Defense cluster fails

Caveat ID Number	Description
CSCve84424	Firepower 2110 Firmware version **MISMATCH** error message after upgrade
CSCve84629	Add code to reread **/etc/sf/devicecap.conf** file when moving to local management
CSCve89196	Double byte characters are not rendered correctly for Identity Policy Name and description
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
CSCve95168	Unicode file support over SMB on Firepwer Threat Defense
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
CSCvf01103	SNMP Username on Platform Settings accepts whitespace characters alone as name
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
CSCvf09949	Incorrect access control rule is matched in FTD when it is setup in **passive** mode.
CSCvf10781	SFDataCorrelator segfaults repeatedly when processing SSL certificate details
CSCvf12124	Third Party Vulnerability Maps won't save
CSCvf14190	M**ultiple routes with same metric or gateway exists** error when configuring ECMP
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 **Do Not Decrypt** SSL rules may be blocked
CSCvf22098	Management interface bootstrap fails with IPv6 only configuratiom and no available DHCPv4 servers
CSCvf30502	Documentation has incorrect info for Max Response Length on Client-Level FTP Options.

Caveat ID Number	Description
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
CSCvf40350	Static route checking is too restrictive
CSCvf41244	ACT LEDS do not reflect the correct high availability states of the devices
CSCvf43107	Estreamer Cores - SSLCert length handling
CSCvf50819	AS Path prepend command truncated while deployed
CSCvf52744	cannot activate correlation policy with malware event by network based with file name as condition
CSCvf55850	access-list rules missing after policy deployment on Firepower Threat Defense
CSCvf57891	Need documentation how to view available OS fingerprint in VDB
CSCvf62276	Missing IP address in AMP cloud malware events
CSCvf74015	After a Manual Sync of Smart License, upgrade from 6.2.0-363 to 6.2.2-66 fails
CSCvf74292	Outage caused by process exiting