# ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Cisco Adaptive Security Appliances (ASA) 5500-X, Industrial Security Appliances (ISA) 3000 and ASA Virtual (ASAv) Version 9.16

---

**Maintenance Update of Cisco Adaptive Security Appliances (ASA) 5500-X, Industrial Security Appliances (ISA) 3000 and ASA Virtual (ASAv) Version 9.16**

**Maintenance Report Number:** CCEVS-VR-VID11257-2023

**Date of Activity**: 10 May 2023

**References:**

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016.
- Impact Analysis Report for Cisco Adaptive Security Appliances (ASA) 5500-X, Industrial Security Appliances (ISA) 3000 and ASA Virtual (ASAv) Version 9.16, Version 1.1, 04/27/2023.
- PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways (CFG_NDcPP-FW-VPNGW_V1.1
  The PP-Configuration includes the following components:
  - Base-PP: Collaborative Protection Profile for Network Devices, (CPP_ND_V2.2E)
  - PP-Module for Stateful Traffic Filter Firewalls, (MOD_CPP_FW_1.4E)
  - PP-Module for Virtual Private Network (VPN) Gateways, (MOD_VPNGW_V1.1)

**Documentation updated**:

| Evidence Identification | Effect on Evidence/ Description of Changes |
|---|---|
| **Evaluated Security Target:**<br>Cisco Adaptive Security Appliances (ASA) 5500-X, Industrial Security Appliances (ISA) 3000 and ASA Virtual (ASAv) Version 9.16 Security Target Version 0.7, Date 05/06/2022 | **Current Maintained Security Target:**<br>Cisco Adaptive Security Appliances (ASA) 5500-X, Industrial Security Appliances (ISA) 3000 and ASA Virtual (ASAv) Version 9.16 Security Target, Version 0.9, 02/13/2023<br><br>The Security Target was updated to identify the new hardware platforms. |
| **Evaluated Common Criteria Guidance Documentation:**<br>Cisco Adaptive Security Appliance (ASA) 9.16 Preparative Procedures & Operational User Guide for the Common Criteria Certified configuration, Version 0.4, 03/30/2022 | **Maintained Common Criteria Guidance Documentation:**<br>Cisco Adaptive Security Appliance (ASA) 9.16 Preparative Procedures & Operational User Guide for the Common Criteria Certified configuration, Version 0.5, 2/22/2023<br>The Guidance document was updated to identify the new hardware platforms. |

**Assurance Continuity Maintenance Report:**

The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence consists of the Security Target, the Administrative Guide, and the Impact Analysis Report (IAR). The ST and guide document were updated, the IAR was new.

**Changes to TOE:**

Two new hardware platforms were added:

- Intel Xeon E-2254ML (Coffee Lake)
- Intel Xeon D-1539 (Broadwell)

The tested/evaluated version runs on these new platforms. The algorithm certificate, A2428, has been updated to include these two platforms specifically. Each platform has been included in the certificate on the claimed ESXi 6.7 and 7.0.

**Changes to Evaluation Documents:**

1. Security Target – The Security Target has been Updated to identify the new hardware platforms
2. Guidance document – The Admin Guide has been Updated to identify the new hardware platforms.

**Software Changes**

Software changes are identified and described in the following table that lists the resolved bugs. For any that appear security relevant, more detail has been added.

| Identifier | Headline | Security Analysis |
|---|---|---|
| CSCvw82067 | ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic | FTD not in the evaluation scope |
| CSCvx56021 | FTD: CTS SGT propagation gets enabled after reload | FTD not in the evaluation scope |
| CSCvy50598 | BGP table not removing connected route when interface goes down | BGP table not evaluated in scope of the evaluation |
| CSCvy67765 | FTD VTI reports TUNNEL_SRC_IS_UP false despite source interface is up/up and working | FTD not in the evaluation scope |
| CSCvy73130 | FP4100 platform: Active-Standby changed to dual Active after running "show conn" command | FP4100 not in the evaluation scope |
| CSCvy86817 | Cruz ASIC CLU filter has the incorrect src/dst IP subnet when a custom CCL IP subnet is set | FP9300 not in the evaluation scope |
| CSCvz09106 | Cisco ASA and FTD Software SSL VPN Denial of Service Vulnerability | A vulnerability in the implementation of the Datagram TLS (DTLS) protocol in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause high CPU utilization, resulting in a denial of service (DoS) condition. – DTLS not in the scope of the evaluation |
| CSCvz36903 | ASA traceback and reload while allocating a new block for cluster keepalive packet | ASA crashing not security relevant |
| CSCvz60142 | ASA/FTD stops serving SSL connections | Affected platforms are only FPR1xxx – these are not in the evaluation scope |
| CSCvz68713 | PLR license reservation for ASAv5 is requesting ASAv10 | ASAv5 not in the evaluation scope |
| CSCvz69729 | Unstable client processes may cause LINA zmqio traceback on FTD | FTD not in the evaluation scope |

| Identifier | Headline | Security Analysis |
|---|---|---|
| CSCvz71596 | "Number of interfaces on Active and Standby are not consistent" should trigger warning syslog | Reporting of number of devices is not security relevant |
| CSCvz88020 | ASAv: coredumpfsys is formatted during bootup | In ASAv deployments, coredumpfsys file system is being formatted during every bootup and as a result, cores are not getting dumped when device crashes. – Not security relevant but helpful for debug purposes in the real world |
| CSCwa03341 | Standby's sub interface mac doesn't revert to old mac with no mac-address command | Symptom:Standby's sub interface mac doesn't revert to old mac with no mac-address command<br><br>Conditions:When manual mac address is removed with no mac-address command , ASAv are in HA<br><br>High availability was not in the evaluation scope. |
| CSCwa36535 | Standby unit failed to join failover due to large config size. | Rebooting is no a security relevant issue |
| CSCwa43311 | Snort blocking and dropping packet, with bigger size(1G) file download | IPS was not included in the evaluation scope. |
| CSCwa47737 | ASA/FTD may hit a watchdog traceback related to snmp config writing | SNMP was not included in the evaluation scope. |
| CSCwa49480 | SNMP OID , stop working after around one hour and a half - FTD | SNMP was not included in the evaluation scope. |
| CSCwa59907 | LINA observed traceback on thread name "snmp_client_callback_thread" | LINA was not included in the evaluation scope. (FTD related) |
| CSCwa61361 | ASAv traceback when SD_WAN ACL enabled, then disabled (or vice-versa) in PBR | Symptom:ASA traceback and reload when inactive/active keyword used in the access-list in case of PBR and corresponding Access-list used by it.<br><br>Conditions:First seen on ASA5516 running version 9.14.2 & can be seen any other releases also<br><br>Crash is seen when the ACL used/added in a PBR, is first disabled, and then enabled (or vice-versa) repeatedly.<br><br>Workaround:Instead of using the active/inactive option for the access list, it is advisable to remove the access-list cli when not needed anymore and add back when needed.<br><br>Crash is not security relevant and workaround is provided. |
| CSCwa62025 | IPv6: Some of egress interfaces of global and user vrf routes are missing in asp table | Symptom: IPV6 Traffic is not hitting on some egress interfaces of user vrf due to routes missing in asp table<br><br>This is a functional issue and not a security issue. |
| CSCwa68552 | All type-8 passwords are lost upon upgrade from ASA 9.12-9.15 to 9.16, failover gets disabled | The evaluation did not consider upgrade configurations. |
| CSCwa72530 | FTD: Time gap/mismatch seen when new node joins a Cluster Control node under history | IPS was not included in the evaluation scope. |
| CSCwa72929 | SNMPv3 polling may fail using privacy algorithms AES192/AES256 | SNMP was not included in the evaluation scope. |

| Identifier | Headline | Security Analysis |
|---|---|---|
| CSCwa73172 | ASA reload and traceback in Thread Name: PIX Garbage Collector | Symptom:ASA HA pair both nodes reloaded due to Lina traceback.<br><br>The ASA traceback is seen in PIX garbage collector.<br><br>High availability was not included in the evaluation scope. |
| CSCwa75966 | ASA: Reload and Traceback in Thread Name: Unicorn Proxy Thread with Page fault: Address not mapped | Conditions: WebVPN enable<br><br>WebVPN was not included in the evaluation scope |
| CSCwa82850 | ASA Failover does not detect context mismatch before declaring joining node as "Standby ready" | Failover was not included in the evaluation scope |
| CSCwa95079 | ASA/FTD Traceback and reload due to NAT configuration | Failover was not included in the evaluation scope |
| CSCwa97917 | ISA3000 in boot loop after powercycle | Symptom: ISA3000 stuck in boot loop after reboot<br><br>Conditions:ISA-3000-4C-X running FTD 7.0.1 and patch applied to fix the shutdown feature.<br><br>FTD was not included in the evaluation scope |
| CSCwa99931 | ASA/FTD: Tuning of update_mem_reference process | Symptom:Despite the fix to CSCvz61658, CPU hogs in update_mem_reference can still be observed in some cases. This defect serves as a tuning of the update_mem_reference process to further decrease CPU hog durations and frequency.<br><br>Performance was not included in the evaluation scope |
| CSCwb02060 | snmp-group host with Invalid host range and subnet causing traceback and reload | SNMP was not included in the evaluation scope |
| CSCwb03704 | ASA/FTD datapath threads may run into deadlock and generate traceback | Symptom: ASA/FTD datapath threads may run into deadlock and generate traceback.<br><br>Performance was not included in the evaluation scope |
| CSCwb04000 | ASA/FTD: DF bit is being set on packets routed into VTI | Symptom: After upgrading to 9.16 large UDP fragments destined for a VTI interface, and that would require a second fragmentation after encryption, are dropped.<br><br>Workaround: Explicitly configuring the tunnel source to clear the df bit (instead of the default behavior which is copy) allows the packets to be fragmented after encryption<br><br>This is a functional issue on receiving packets. The TOE defaults to dropping packets which is secure. A workaround is provided for larger UDP packets but is not recommended and no code change was made. |
| CSCwb05291 | Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability | A vulnerability in the packaging of Cisco Adaptive Security Device Manager (ASDM) images and the validation of those images by Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker with administrative privileges to upload an ASDM image |

| Identifier | Headline | Security Analysis |
|---|---|---|
| | | that contains malicious code to a device that is running Cisco ASA Software.<br><br>This vulnerability is due to insufficient validation of the authenticity of an ASDM image during its installation on a device that is running Cisco ASA Software. An attacker could exploit this vulnerability by installing a crafted ASDM image on the device that is running Cisco ASA Software and then waiting for a targeted user to access that device using ASDM. A successful exploit could allow the attacker to execute arbitrary code on the machine of the targeted user with the privileges of that user on that machine.<br><br>Notes:To successfully exploit this vulnerability, the attacker must have administrative privileges on the device that is running Cisco ASA Software.<br><br>Potential targets are limited to users who manage the same device that is running Cisco ASA Software using ASDM<br><br>This patch will be required to use the ASDM for management. The ASDM is not part of the TOE but is a tool an administrator can use. The bug requires an evil admin which is contrary to the NDcPP assumptions. |
| CSCwb06847 | ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543' | Symptom: ASA/FTD may traceback and reload citing Thread Name 'DATAPATH-9-11543' as the faulting thread<br><br>Tracing was not included in the evaluation scope |
| CSCwb07908 | Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0 | Symptom: Standby ASA or FTD unit sends DNS queries with source IP of 0.0.0.0<br><br>This is a configuration error. The workaround is to configure the standby IP address for DNS server facing interface |
| CSCwb07981 | Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server | FTD was not included in the evaluation scope |
| CSCwb08644 | ASA/FTD traceback and reload at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test | Symptom: ASA/FTD crashes after running out of memory and memory alloc failing for SA.<br><br>Conditions: The issue was found during scaled tests using a firewall with AnyConnect, site-to-site VPNs and SNMP configured<br><br>This is a usability issue and not a security issue. Also SNMP is outside the evaluation scope. |
| CSCwb16920 | CPU profile cannot be reactivated even if previously active memory tracking is disabled | Symptom: On Firepower 2100, activation of CPU profiling tool while memory tracking is already running results in error<br><br>FTD was not included in the evaluation scope. |

| Identifier | Headline | Security Analysis |
|---|---|---|
| CSCwb17187 | SNMP cores are generated every minute while running snmpwalk on HA | SNMP was not included in the evaluation scope |
| CSCwb17963 | Unable to identify dynamic rate liming mechanism & not following msg limit per/sec at syslog server. | Symptom: Observed more than configured message count at syslog server side when dynamic rate limiting mechanism triggered.<br><br>Conditions: When Dynamic rate limiting mechanism triggered.<br><br>Dynamic rate limiting is a functional and not security mechanism. Also, all records are at syslog – only count is inaccurate. |
| CSCwb19648 | SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels. | FTD was not included in the evaluation scope |
| CSCwb24039 | ASA traceback and reload on routing | Symptom: Traceback on Lina ASA, the problem was seen only once.<br><br>Cisco deemed this not an issue. It could not be reproduced. |
| CSCwb25809 | Single Pass - Traceback due to stale ifc | Symptom: Crash during single pass processing<br><br>Traceback was not included in the evaluation scope |
| CSCwb28123 | FTD HA deployment fails with error "Deployment failed due to major version change on device" | FTD not in the evaluation scope |
| CSCwb31551 | When inbound packet contains SGT header, FPR2100 cannot distribute properly per 5 tuple | FTD was not included in the evaluation scope |
| CSCwb31699 | Primary takes active role after reload | Symptom: When primary is standby and secondary is active and reload the primary(standby), then primary becomes active and secondary becomes standby<br><br>Failover functionality was not included in the evaluation scope |
| CSCwb32841 | NAT (any,any) statements in-states the failover interface and resulting on Split Brain events | Failover functionality was not included in the evaluation scope |
| CSCwb40001 | Long delays when executing SNMP commands | SNMP functionality was not included in the evaluation scope |
| CSCwb43018 | Implement SNP API to check ifc and ip belongs to HA LU or CMD interface | Symptom: This is an enhancement change on the HA code, as a complementary fix for an effective solution of defect CSCwb32841.<br><br>Failover functionality was not included in the evaluation scope |
| CSCwb50405 | ASA/FTD Traceback in crypto hash function | Symptom: System traceback and reload due to an issue in the crypto function.<br><br>Conditions: ASA/FTD with SSL crypto configurations & WebVPN DTLS enabled.<br><br>WebVPN DTLS was not included in the evaluation scope. |

| Identifier | Headline | Security Analysis |
|---|---|---|
| CSCwb51707 | ASA Traceback and reload in process name: lina | Traceback functionality was not included in the evaluation scope |
| CSCwb53172 | FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated | FTD functionality was not included in the evaluation scope |
| CSCwb53191 | Certificate validation fails post upgrade to 9.17.1 | This is a later version of the ASA product |
| CSCwb53328 | ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url | Traceback functionality was not included in the evaluation scope |
| CSCwb54791 | ASA DHCP server fails to bind reserved address to Linux devices | Symptom: ASA DHCP server fails to bind the reserved IP address for Linux devices, offering an IP address of the common DHCP pool.<br><br>Workaround:Prepend the hardware type to the mac address on the DHCP reserved configuration, and remove the last 2 digits.<br><br>This is a functional issue but the fix is a manual process and no product changes have been made. |
| CSCwb57615 | Configuring pbr access-list with line number failed. | Symptom: Configuring pbr access-list with 'line' causes error and the config is rejected with the following error message:<br><br>ciscoasa/actNoFailover(config)# access-list pbr line 1 permit ip any host 1.1.1.1<br><br>ERROR: ACL is associated with route-map and inactive not supported, instead remove the acl<br><br>Workaround: Don't include 'line' parameter in access-list.<br><br>The fix is a manual process and no product changes have been made. |
| CSCwb59465 | ASA/FTD may traceback (watchdog) and reload when generating a syslog from the VPN Failover subsystem | Traceback functionality was not included in the evaluation scope |
| CSCwb59488 | ASA/FTD Traceback in memory allocation failed | Traceback functionality was not included in the evaluation scope |
| CSCwb67040 | FP4112\|4115 Traceback & reload on Thread Name: netfs_thread_init | FTD and Traceback functionality were not included in the evaluation scope |
| CSCwb68642 | ASA traceback in Thread Name: SXP CORE | Traceback functionality was not included in the evaluation scope |
| CSCwb69503 | ASA unable to configure aes128-gcm@openssh.com when FIPS enabled | The evaluation just covered AES-CBC for SSHS. This is expected behavior. |
| CSCwb71460 | ASA traceback in Thread Name: fover_parse and triggered by snmp related functions | Traceback functionality was not included in the evaluation scope |
| CSCwb73248 | FW traceback in timer infra / netflow timer | Traceback functionality was not included in the evaluation scope |

| Identifier | Headline | Security Analysis |
|---|---|---|
| CSCwb74571 | PBR not working on ASA routed mode with zone-members | Symptom: ASA in routed mode and data-interfaces are part of zone-members.<br><br>PBR is configured on all the data-interfaces with floating default routes. packet tracer output is showing that the is traffic hitting on the correct PBR and is allowed but ASA is dropping packets due to 'tcp-not-syn"<br><br>When we remove the zone-member configuration for the data-interfaces then it works and we don't see any TCP RST packets and no ASP drops.<br><br>Workaround: Configure - timeout floating-conn 0:00:30(default floating conn timeout is 0:00:00).<br><br>The fix is a manual process and no product changes have been made |
| CSCwb79812 | RIP is advertising all connected Anyconnect users and not matching route-map for redistribution | Symptoms: Cisco Adaptive Security Appliance Software Version 9.12(4) SSP Operating System Version 2.6(1.198) Device Manager Version 7.15(1)150<br><br>Not applicable – older version of ASA |
| CSCwb80559 | FTD offloads SGT tagged packets although it should not | FTD was not included in the evaluation scope |
| CSCwb80862 | ASA/FTD proxy arps any traffic when using the built-in 'any' object in translated destination | FTD was not included in the evaluation scope |
| CSCwb82796 | ASA/FTD firewall may traceback and reload when tearing down IKE tunnels | Traceback functionality was not included in the evaluation scope |
| CSCwb83388 | ASA HA Active/standby tracebacks seen approximately every two months. | Traceback functionality was not included in the evaluation scope |
| CSCwb83691 | ASA/FTD traceback and reload due to the initiated capture from FMC | Traceback functionality was not included in the evaluation scope |
| CSCwb85633 | Snmpwalk output of memory does not match show memory/show memory detail | SNMP functionality was not included in the evaluation scope |
| CSCwb87498 | Lina traceback and reload during EIGRP route update processing. | Traceback functionality was not included in the evaluation scope |
| CSCwb88651 | Cisco ASA and FTD Software RSA Private Key Leak Vulnerability | Impacts these products:<br><br>• ASA 5506-X with FirePOWER Services<br>• ASA 5506H-X with FirePOWER Services<br>• ASA 5506W-X with FirePOWER Services<br>• ASA 5508-X with FirePOWER Services<br>• ASA 5516-X with FirePOWER Services<br>• Firepower 1000 Series Next-Generation Firewall<br>• Firepower 2100 Series Security Appliances<br>• Firepower 4100 Series Security Appliances<br>• Firepower 9300 Series Security Appliances<br>• Secure Firewall 3100 |

| Identifier | Headline | Security Analysis |
|---|---|---|
| | | None of these products are in the evaluation. |
| CSCwb89963 | ASA Traceback & reload in thread name: Datapath | Traceback functionality was not included in the evaluation scope |
| CSCwb90074 | ASA: Multiple Context Mixed Mode SFR Redirection Validation | This bug deals with ASA FirePOWER Inline Tap Monitor-Only Mode<br><br>FirePOWER products are not in the evaluation. |
| CSCwb90532 | ASA/FTD traceback and reload on NAT related function nat_policy_find_location | Traceback functionality was not included in the evaluation scope |
| CSCwb92709 | We can't monitor the interface via "snmpwalk" once interface is removed from context. | Symptom: Once we remove any interface from context, we can't monitor that interface via snmpwalk.<br><br>Workaround:Write mem and reload is a workaround for this issue.<br><br>The fix is a manual process and no product changes have been made. |
| CSCwb93932 | ASA/FTD traceback and reload with timer services assertion | Traceback functionality was not included in the evaluation scope |
| CSCwb94190 | ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled. | Symptom: ASA may spontaneously reboot when applying ACLs with FIPS and forward-reference enabled. This appears to be due to a temporary FIPS self-test failure.<br><br>The “forward-reference” feature is outside the scope of the evaluation. In 9.16.x the feature is disabled by default.<br><br>The impact of the now-resolved bug actually showed that other security relevant features were working as intended, i.e. to reboot the TOE in the event of FIPS self-test failure. |
| CSCwb94312 | Unable to apply SSH settings to ASA version 9.16 or later | Cisco unable to reproduce – recommend reloading. |
| CSCwb97251 | ASA/FTD may traceback and reload in Thread Name 'ssh' | Traceback functionality was not included in the evaluation scope |
| CSCwc02488 | ASA/FTD may traceback and reload in Thread Name 'None' | Traceback functionality was not included in the evaluation scope |
| CSCwc03069 | Interface internal data0/0 is up/up from cli but up/down from SNMP polling | SNMP was not included in the evaluation scope |
| CSCwc07262 | Standby ASA goes to booting loop during configuration replication after upgrade to 9.16(3). | Failover was not included in the evaluation scope |
| CSCwc09414 | ASA/FTD may traceback and reload in Thread Name 'ci/console' | Traceback functionality was not included in the evaluation scope |
| CSCwc10483 | ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread | Traceback functionality was not included in the evaluation scope |
| CSCwc10792 | ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete | Symptom: IPSEC debugs may fail to list the reason for peer change of address or timer delete. |

| Identifier | Headline | Security Analysis |
|---|---|---|
| | | IPSEC ERROR: Failed to send the message to IKE<br><br>Conditions: IPSEC debugs being utilized<br><br>This update fixed a bug that was causing some debug details to not be shown on the console in a few cases. There was no impact to the syslog-formatted messages that are written to the local logging buffer and transmitted to the remote audit server. There is no change in SFR claims due to this bug fix. |
| CSCwc11511 | FTD: SNMP failures after upgrade to 7.0.2 | FTD was not included in the evaluation scope |
| CSCwc11597 | ASA tracebacks after SFR was upgraded to 6.7.0.3 | Traceback functionality was not included in the evaluation scope |
| CSCwc11663 | ASA traceback and reload when modifying DNS inspection policy via CSM or CLI | Traceback functionality was not included in the evaluation scope |
| CSCwc13017 | FTD/ASA traceback and reload at at ../inspect/proxy.h:439 | Traceback functionality was not included in the evaluation scope |
| CSCwc13994 | ASA - Restore not remove the new configuration for an interface setup after backup | Symptom: For a sub-interface configured after the backup has been done, the configuration is not clearing by restore command.<br><br>Workaround: use write ease to clean the running config.<br><br>The fix is a manual process and no product changes have been made. |
| CSCwc18312 | "show nat pool cluster" commands run within EEM scripts lead to traceback and reload | Workaround: Use the show nat pool cluster commands manually not within an EEM script<br><br>The fix is a manual process and no product changes have been made. |
| CSCwc18524 | ASA/FTD Voltage information is missing in the commnad "show environment" | This is non-security relevant data in a show command. |
| CSCwc23356 | ASA/FTD may traceback and reload in Thread Name 'DATAPATH-20-7695' | Traceback functionality was not included in the evaluation scope |
| CSCwc23695 | ASA/FTD can not parse UPN from SAN field of user's certificate | Symptom: "Unknown" is visible in radius debugs when fetching username from SAN field of a user's certificate for authorization<br><br>Conditions: having UPN in SAN field and subject name is empty in certificate of a user.<br><br>The fix addresses the bug where "Unknown" is visible in RADIUS debugs when fetching User Principle Name (UPN) username from SAN field of a user's certificate for authorization. Use of User Principle Name (UPN) username in client certificates was outside the scope of the evaluation. |
| CSCwc24906 | ASA/FTD traceback and reload on Thread id: 1637 | Traceback functionality was not included in the evaluation scope |

| Identifier | Headline | Security Analysis |
|---|---|---|
| CSCwc26648 | FTD Traceback and reload in process name lina | FTD was not included in the evaluation scope |
| CSCwc27797 | ASA mgmt ip cannot be released | This is an FTD issue.<br>FTD was not included in the evaluation scope |
| CSCwc28334 | Cisco ASA and FTD Software RSA Private Key Leak Vulnerability | Same as previous RSA bug – devices from evaluation not impacted. |
| CSCwc28532 | 9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing | Symptom: low available 9344 blocks resulting in ASP drops due to Snort Busy<br><br>This is applicable to NGIPS which was not in this evaluation. |
| CSCwc28806 | ASA Traceback and Reload on process name Lina | Traceback functionality was not included in the evaluation scope |
| CSCwc28928 | ASA: SLA debugs not showing up on VTY sessions | Tested on an ASAv running 9.14(1)30<br><br>This is an older version of the TOE and in any case, the logs are not part of the requited audits. |
| CSCwc32246 | NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used | Symptom:NAT64 fails to translate IPv6 to IPv4 with the embedded IPv4 address as seen in the packet tracer examples.<br><br>This has a manual workaround and no product changes were made. |
| CSCwc36905 | ASA traceback and reload due to "Heap memory corrupted at slib_malloc.c | Symptom: The device, in HA, may traceback and reload due to heap memory corruption for the following reason:<br><br>"Heap memory corrupted: (next_pinuse(p)) is false") at slib_malloc.c:5996<br><br>High availability and traceback were not included in the evaluation scope |
| CSCwc38567 | ASA/FTD may traceback and reload while executing SCH code | Traceback functionality was not included in the evaluation scope |
| CSCwc40381 | ASA : HTTPS traffic authentication issue with Cut-through Proxy enabled | Symptom: ++ ASA enabled with Cut-through Proxy, after upgrading to 9.16 and above fails to authenticate HTTPS traffic, HTTP traffic is not impacted.<br><br>The “Cut-through Proxy” feature (an authentication proxy functionality) is outside the scope of the evaluation. |
| CSCwc44289 | FTD - Traceback and reload when performing IPv4 <> IPv6 NAT translations | FTD was not included in the evaluation scope |
| CSCwc45108 | ASA/FTD: GTP inspection causing 9344 sized blocks leak | Symptom:<br><br>When GTP inspection is enabled with default permit-error parameter and IP fragments are sent over GTP tunnels, 9344 block depletion is seen. By default, all invalid packets or packets that failed parsing are dropped. |

| Identifier | Headline | Security Analysis |
|---|---|---|
| | | GTP correctness was not included in the evaluation scope. Also, no product changes were made – a manual workaround was recommended. |
| CSCwc45397 | ASA HA - Restore in primary not remove new interface configuration done after backup | High availability and traceback were not included in the evaluation scope |
| CSCwc48375 | Inbound IPSEC SA stuck inactive - many inbound SPIs for one outbound SPI in "show crypto ipsec sa" | Symptom: Apart from excessive logging rate no impact for VPN traffic observed.<br><br>Conditions:Crypto map based L2L VPN using IKEv1 or IKEv2.<br><br>Problem seen on FMC managed FTD on Firepower 2140<br><br>Workaround:Reload of the device (in case of single device) or both devices at the same time (in case of failover pair) will remove the stuck IPSEC SAs.<br><br>FTD was not included in the evaluation scope. Also, no product changes were made – a manual workaround was recommended |
| CSCwc49095 | ASA/FTD may traceback and reload in Thread Name 'lina' | Traceback functionality was not included in the evaluation scope. |
| CSCwc50887 | FTD - Traceback and reload on NAT IPv4<>IPv6 for UDP flow redirected over CCL link | FTD and Traceback functionality were not included in the evaluation scope |
| CSCwc50891 | MPLS tagging removed by FTD | FTD was not included in the evaluation scope. |
| CSCwc51326 | FXOS-based Firepower platform showing 'no buffer' drops despite high values for RX ring watermarks | FirePOWER was not included in the evaluation scope. |
| CSCwc52351 | ASA/FTD Cluster Split Brain due to NAT with "any" and Global IP/range matching broadcast IP | Clusters were not included in the evaluation scope |
| CSCwc53280 | ASA parser accepts incomplete network statement under OSPF process and is present in show run | Symptom: ASA parser accepts incomplete network statement under OSPF process and is present in show run.<br><br>This is a display error and not a security issue. Also, no product changes were made – a manual workaround was recommended |
| CSCwc54217 | syslog related to failover is not outputted in FPR2140 | FPR2140 was not included in the evaluation scope |
| CSCwc54984 | IKEv2 rekey - Responding Invalid SPI for the new SPI received right after Create_Child_SA response | Symptom: The IPSEC VPN tunnel flaps intermittently during a rekey request from Cisco ASA. The VPN recovers in a couple of minutes on its own, however, there is an outage for a couple of minutes when the tunnel is down.<br><br>The bug could cause an IPsec VPN tunnel to flaps intermittently during a rekey request from Cisco ASA causing an outage for a couple of minutes after which the tunnel recovers on its own. This is a useability issue and not a security issue. |
| CSCwc60037 | ASA fails to rekey with IPSEC ERROR: Failed to allocate an outbound hardware context | This was a specific customer error and not a general issue. |

| Identifier | Headline | Security Analysis |
|---|---|---|
| CSCwc61912 | ASA/FTD OSPFv3 does not generate messages Type 8 LSA for IPv6 | Symptom: After an ospfv3 event in the network, FTD is not able to generate LSA Type 8 messages.<br><br>FTD was not included in the evaluation scope |
| CSCwc70962 | FTD/ASA "Write Standby" enables ECDSA ciphers causing AC SSLv3 handshake failure | Symptom: - After upgrading to 9.16.2.14, and running the command "wr standby" on the active unit, accepted SSL ciphers would change.<br><br>- We can see that the configuration stays the same, but "show ssl ciphers" will show different outputs after the "wr standby" command<br><br>The wr standby command was not in the evaluation. |
| CSCwc73224 | Call home configuration on standby device is lost after reload | This is a FirePOWER issue. FirePOWER was not included in the evaluation scope. |
| CSCwc74858 | FTD - Traceback in Thread Name: DATAPATH | FTD was not included in the evaluation scope |
| CSCwc79366 | During the deployment time, device got stuck processing the config request. | This was a specific customer error and not a general issue. |
| CSCwc81960 | Unable to configure 'match ip address' under route-map when using object-group in access list | Symptom: Unable to configure 'match ip address' under route-map when using object-group in access list<br><br>Conditions: This behaviour is observed only on ASA 9.18.x and it should not affect 9.17.x and below<br><br>This bug impacts a later product than was evaluated. |
| CSCwc88897 | ASA traceback and reload due to null pointer in Umbrella after modifying DNS inspection policy | Traceback functionality was not included in the evaluation scope. |
| CSCwc94085 | Unable to establish DTLSv1.2 with FIPS enabled after upgrade from 6.6.5. | DTLS is not included in the evaluation so this is expected behavior. |
| CSCwd03810 | ASA Custom login page is not working through webvpn after an upgrade | Symptom: After upgrading ASA to 9.16, customers cannot log into the clientless portal.<br>Conditions: ASA with webvpn functionality.<br><br>The webvpn was not included in the evaluation scope. |

**Regression Testing:**

The Development team regression tested the ASAv 9.16 software on the added platform to ensure it performed correctly. The Development Testing Team (Dev Test Team) performs regular testing on interim images to validate any bug fixes or to confirm that new functionality has been correctly incorporated into images being built for customer use. For maintenance releases, additional regression testing is also performed using the Automated Regression Facility (ARF). The ARF is a collection of automated scripts that test the functionality of built images. The test scripts used within ARF are developed in conjunction with the associated Dev Test group.

**Vulnerability Analysis:**

The public search was updated from 06/07/2022 on 3/13/2023 and 4/27/2023. No new public vulnerabilities were discovered that are applicable to the product.

**Conclusion:**

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor. No functionality, as defined in the SFRs, was impacted, and all software updates were bug fixes. Thus, there were no changes to the security functionality or the SFRs identified in the Security Target. Therefore, CCEVS agrees that the original assurance is maintained for the product.