



Release Notes for the Cisco ASA Series, 9.4(x)

First Published: 2015-03-23

Last Modified: 2017-04-17

Release Notes for the Cisco ASA Series, 9.4(x)

This document contains release information for Cisco ASA software Version 9.4(x).

Important Notes

- Potential Traffic Outage (9.4(3.11) through 9.4(4))—Due to bug [CSCvd78303](#), the ASA may stop passing traffic after 213 days of uptime. The effect on each network will be different, but it could range from an issue of limited connectivity to something more extensive like an outage. You must upgrade to a new version without this bug, when available. In the meantime, you can reboot the ASA to gain another 213 days of uptime. Other workarounds may be available. See Field Notice [FN-64291](#) for affected versions and more information.
- For the ASA 5506H-X, when you upgrade to ASA Version 9.5(2), the correct licensing level is applied. Earlier ASA versions apply the same licensing as the ASA 5506-X base license. For earlier versions, you can contact Cisco to receive the ASA 5506-X Security Plus license, which is equivalent to the correct ASA 5506H-X base license; or simply upgrade to 9.5(2).
- Unified Communications Phone Proxy and Intercompany Media Engine Proxy are deprecated—In ASA Version 9.4, the Phone Proxy and IME Proxy are no longer supported.
- Elliptic curve cryptography for SSL/TLS—When an elliptic curve-capable SSL VPN client connects to the ASA, the elliptic curve cipher suite will be negotiated, and the ASA will present the SSL VPN client with an elliptic curve certificate, even when the corresponding interface has been configured with an RSA-based trustpoint. To avoid having the ASA present a self-signed SSL certificate, the administrator needs to remove the corresponding cipher suites using the **ssl cipher** command. For example, for an interface configured with an RSA trustpoint, the administrator can execute the following command so that only RSA based ciphers are negotiated:

```
ssl cipher tlsv1.2 custom
"AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:
DES-CBC-SHA:RC4-SHA:RC4-MD5"
```

- The RSA toolkit version used in ASA 9.x is different from what was used in ASA 8.4, which causes differences in PKI behavior between these two versions.

For example, ASAs running 9.x software allow you to import certificates with an Organizational Name Value (OU) field length of 73 characters. ASAs running 8.4 software allow you to import certificates with an OU field name of 60 characters. Because of this difference, certificates that can be imported in ASA 9.x will fail to be imported to ASA 8.4. If you try to import an ASA 9.x certificate to an ASA running version 8.4, you will likely receive the error, "ERROR: Import PKCS12 operation failed.

System Requirements

This section lists the system requirements to run this release.

ASA and ASDM Compatibility

For information about ASA/ASDM software and hardware requirements and compatibility, including module compatibility, see [Cisco ASA Compatibility](#).

VPN Compatibility

For VPN compatibility, see [Supported VPN Platforms, Cisco ASA 5500 Series](#).

New Features

This section lists new features for each release.



Note New, changed, and deprecated syslog messages are listed in the syslog message guide.

New Features in ASA 9.4(4.5)

Released: April 3, 2017



Note Verion 9.4(4) was removed from Cisco.com due to bug [CSCvd78303](#).

There are no new features in this release.

New Features in ASA 9.4(3)

Released: April 25, 2016

Feature	Description
Firewall Features	
Connection holddown timeout for route convergence	You can now configure how long the system should maintain a connection when the route used by the connection no longer exists or is inactive. If the route does not become active within this holddown period, the connection is freed. You can reduce the holddown timer to make route convergence happen more quickly. However, the 15 second default is appropriate for most networks to prevent route flapping. We added the following command: timeout conn-holddown
Remote Access Features	

Feature	Description
Configurable SSH encryption and HMAC algorithm.	<p>Users can select cipher modes when doing SSH encryption management and can configure HMAC and encryption for varying key exchange algorithms.</p> <p>We introduced the following commands: ssh cipher encryption, ssh cipher integrity.</p> <p><i>Also available in 9.1(7).</i></p>
HTTP redirect support for IPv6	<p>When you enable HTTP redirect to HTTPS for ASDM access or clientless SSL VPN, you can now redirect traffic sent an to IPv6 address.</p> <p>We added functionality to the following command: http redirect</p> <p><i>Also available in 9.1(7).</i></p>
Monitoring Features	
SNMP engineID sync for Failover	<p>In a failover pair, the SNMP engineIDs of the paired ASAs are synced on both units. Three sets of engineIDs are maintained per ASA—synced engineID, native engineID and remote engineID.</p> <p>An SNMPv3 user can also specify the engineID of the ASA when creating a profile to preserve localized snmp-server user authentication and privacy options. If a user does not specify the native engineID, the show running config output will show two engineIDs per user.</p> <p>We modified the following command: snmp-server user</p>
show tech support enhancements	<p>The show tech support command now:</p> <ul style="list-style-type: none"> • Includes dir all-filesystems output—This output can be helpful in the following cases: <ul style="list-style-type: none"> • SSL VPN configuration: check if the required resources are on the ASA • Crash: check for the date timestamp and presence of a crash file • Removes the show kernel cgroup-controller detail output—This command output will remain in the output of show tech-support detail. <p>We modified the following command: show tech support</p> <p><i>Also available in 9.1(7).</i></p>
Support for the cempMemPoolTable in the CISCO-ENHANCED-MEMPOOL-MIB	<p>The cempMemPoolTable of the CISCO-ENHANCED-MEMPOOL-MIB is now supported. This is a table of memory pool monitoring entries for all physical entities on a managed system.</p> <p>Note The CISCO-ENHANCED-MEMPOOL-MIB uses 64-bit counters and supports reporting of memory on platforms with more than 4GB of RAM.</p> <p>We did not add or modify any commands.</p> <p><i>Also available in 9.1(7).</i></p>

New Features in ASA 9.4(2.145)

Released: November 13, 2015

There are no new features in this release.



Note This release supports only the Firepower 9300 ASA security module.

New Features in ASA 9.4(2)

Released: September 24, 2015

There are no new features in this release.



Note ASAv 9.4(1.200) features are not included in this release.



Note This version does not support the ISA 3000.

New Features in ASA 9.4(1.225)

Released: September 17, 2015



Note This release supports only the Cisco ISA 3000.

Feature	Description
Platform Features	
Cisco ISA 3000 Support	<p>The Cisco ISA 3000 is a DIN Rail mounted, ruggedized, industrial security appliance. It is low-power, fan-less, with Gigabit Ethernet and a dedicated management port. This model comes with the ASA Firepower module pre-installed. Special features for this model include a customized transparent mode default configuration, as well as a hardware bypass function to allow traffic to continue flowing through the appliance when there is a loss of power.</p> <p>We introduced the following commands: hardware-bypass, hardware-bypass manual, hardware-bypass boot-delay, show hardware-bypass</p> <p><i>This feature is not available in Version 9.5(1).</i></p>

New Features in ASA 9.4(1.152)

Released: July 13, 2015



Note This release supports only the ASA on the Firepower 9300.

Feature	Description
Platform Features	
ASA security module on the Firepower 9300	We introduced the ASA security module on the Firepower 9300. Note Firepower Chassis Manager 1.1.1 does not support any VPN features (site-to-site or remote access) for the ASA security module on the Firepower 9300.
High Availability Features	
Intra-chassis ASA Clustering for the Firepower 9300	You can cluster up to 3 security modules within the Firepower 9300 chassis. All modules in the chassis must belong to the cluster. We introduced the following commands: cluster replication delay, debug service-module, management-only individual, show cluster chassis
Licensing Features	
Cisco Smart Software Licensing for the ASA on the Firepower 9300	We introduced Smart Software Licensing for the ASA on the Firepower 9300. We introduced the following commands: feature strong-encryption, feature mobile-sp, feature context

New Features in ASAv 9.4(1.200)

Released: May 12, 2015



Note This release supports only the ASAv.

Feature	Description
Platform Features	
ASAv on VMware no longer requires vCenter support	You can now install the ASAv on VMware without vCenter using the vSphere client or the OVFTool using a Day 0 configuration.
ASAv on Amazon Web Services (AWS)	You can now use the ASAv with Amazon Web Services (AWS) and the Day 0 configuration. Note Amazon Web Services only supports models ASAv10 and ASAv30.

New Features in ASA 9.4(1)

Released: March 30, 2015

Feature	Description
Platform Features	
ASA 5506W-X, ASA 5506H-X, ASA 5508-X, ASA 5516-X	<p>We introduced the ASA 5506W-X with wireless access point, hardened ASA 5506H-X, ASA 5508-X, and ASA 5516-X models.</p> <p>We introduced the following command: hw-module module wlan recover image, hw-module module wlan recover image.</p>
Certification Features	
Department of Defense Unified Capabilities Requirements (UCR) 2013 Certification	<p>The ASA was updated to comply with the DoD UCR 2013 requirements. See the rows in this table for the following features that were added for this certification:</p> <ul style="list-style-type: none"> • Periodic certificate authentication • Certificate expiration alerts • Enforcement of the basic constraints CA flag • ASDM Username From Certificate Configuration • ASDM management authorization • IKEv2 invalid selectors notification configuration • IKEv2 pre-shared key in Hex
FIPS 140-2 Certification compliance updates	<p>When you enable FIPS mode on the ASA, additional restrictions are put in place for the ASA to be FIPS 140-2 compliant. Restrictions include:</p> <ul style="list-style-type: none"> • RSA and DH Key Size Restrictions—Only RSA and DH keys 2K (2048 bits) or larger are allowed. For DH, this means groups 1 (768 bit), 2 (1024 bit), and 5 (1536 bit) are not allowed. <p>Note The key size restrictions disable use of IKEv1 with FIPS.</p> <ul style="list-style-type: none"> • Restrictions on the Hash Algorithm for Digital Signatures—Only SHA256 or better is allowed. • SSH Cipher Restrictions—Allowed ciphers: aes128-cbc or aes256-cbc. MACs: SHA1 <p>To see the FIPS certification status for the ASA, see: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProgress.pdf This PDF is updated weekly.</p> <p>See the Computer Security Division Computer Security Resource Center site for more information: http://csrc.nist.gov/groups/STM/cmvp/inprocess.html</p> <p>We modified the following command: fips enable</p>

Feature	Description
Firewall Features	
Improved SIP inspection performance on multiple core ASAs.	If you have multiple SIP signaling flows going through an ASA with multiple cores, SIP inspection performance has been improved. However, you will not see improved performance if you are using a TLS, phone, or IME proxy. We did not modify any commands.
SIP inspection support for Phone Proxy and UC-IME Proxy was removed.	You can no longer use Phone Proxy or UC-IME Proxy when configuring SIP inspection. Use TLS Proxy to inspect encrypted traffic. We removed the following commands: phone-proxy , uc-ime . We removed the phone-proxy and uc-ime keywords from the inspect sip command.
DCERPC inspection support for ISystemMapper UUID message RemoteGetClassObject opnum3.	The ASA started supporting non-EPM DCERPC messages in release 8.3, supporting the ISystemMapper UUID message RemoteCreateInstance opnum4. This change extends support to the RemoteGetClassObject opnum3 message. We did not modify any commands.
Unlimited SNMP server trap hosts per context	The ASA supports an unlimited number of SNMP server trap hosts per context. The show snmp-server host command output displays only the active hosts that are polling the ASA, as well as the statically configured hosts. We modified the following command: show snmp-server host .
VXLAN packet inspection	The ASA can inspect the VXLAN header to enforce compliance with the standard format. We introduced the following command: inspect vxlan .
DHCP monitoring for IPv6	You can now monitor DHCP statistics and DHCP bindings for IPv6.
ESMTP inspection change in default behavior for TLS sessions.	The default for ESMTP inspection was changed to allow TLS sessions, which are not inspected. However, this default applies to new or reimaged systems. If you upgrade a system that includes no allow-tls , the command is not changed. The change in default behavior was also made in these older versions: 8.4(7.25), 8.5(1.23), 8.6(1.16), 8.7(1.15), 9.0(4.28), 9.1(6.1), 9.2(3.2) 9.3(1.2), 9.3(2.2).
High Availability Features	
Blocking syslog generation on a standby ASA	You can now block specific syslogs from being generated on a standby unit. We introduced the following command: no logging message syslog-id standby .
Enable and disable ASA cluster health monitoring per interface	You can now enable or disable health monitoring per interface. Health monitoring is enabled by default on all port-channel, redundant, and single physical interfaces. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link; it is always monitored. You might want to disable health monitoring of non-essential interfaces, for example, the management interface. We introduced the following command: health-check monitor-interface .

Feature	Description
ASA clustering support for DHCP relay	<p>You can now configure DHCP relay on the ASA cluster. Client DHCP requests are load-balanced to the cluster members using a hash of the client MAC address. DHCP client and server functions are still not supported.</p> <p>We introduced the following command: debug cluster dhcp-relay</p>
SIP inspection support in ASA clustering	<p>You can now configure SIP inspection on the ASA cluster. A control flow can be created on any unit (due to load balancing), but its child data flows must reside on the same unit. TLS Proxy configuration is not supported.</p> <p>We introduced the following command: show cluster service-policy</p>
Routing Features	
Policy Based Routing	<p>Policy Based Routing (PBR) is a mechanism by which traffic is routed through specific paths with a specified QoS using ACLs. ACLs let traffic be classified based on the content of the packet's Layer 3 and Layer 4 headers. This solution lets administrators provide QoS to differentiated traffic, distribute interactive and batch traffic among low-bandwidth, low-cost permanent paths and high-bandwidth, high-cost switched paths, and allows Internet service providers and other organizations to route traffic originating from various sets of users through well-defined Internet connections.</p> <p>We introduced the following commands: set ip next-hop verify-availability, set ip next-hop, set ip next-hop recursive, set interface, set ip default next-hop, set default interface, set ip df, set ip dscp, policy-route route-map, show policy-route, debug policy-route</p>
Interface Features	
VXLAN support	<p>VXLAN support was added, including VXLAN tunnel endpoint (VTEP) support. You can define one VTEP source interface per ASA or security context.</p> <p>We introduced the following commands: debug vxlan, default-mcast-group, encapsulation vxlan, inspect vxlan, interface vni, mcast-group, nve, nve-only, peer ip, segment-id, show arp vtep-mapping, show interface vni, show mac-address-table vtep-mapping, show nve, show vni vlan-mapping, source-interface, vtep-nve, vxlan port</p>
Monitoring Features	
Memory tracking for the EEM	<p>We have added a new debugging feature to log memory allocations and memory usage, and to respond to memory logging wrap events.</p> <p>We introduced or modified the following commands: memory logging, show memory logging, show memory logging include, event memory-logging-wrap</p>
Troubleshooting crashes	<p>The show tech-support command output and show crashinfo command output includes the most recent 50 lines of generated syslogs. Note that you must enable the logging buffer command to enable these results to appear.</p>
Remote Access Features	

Feature	Description
Support for ECDHE-ECDSA ciphers	<p>TLSv1.2 added support for the following ciphers:</p> <ul style="list-style-type: none"> • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 <p>Note ECDSA and DHE ciphers are the highest priority.</p> <p>We introduced the following command: ssl ecdh-group.</p>
Clientless SSL VPN session cookie access restriction	<p>You can now prevent a Clientless SSL VPN session cookie from being accessed by a third party through a client-side script such as Javascript.</p> <p>Note Use this feature only if Cisco TAC advises you to do so. Enabling this command presents a security risk because the following Clientless SSL VPN features will not work without any warning.</p> <ul style="list-style-type: none"> • Java plug-ins • Java rewriter • Port forwarding • File browser • Sharepoint features that require desktop applications (for example, MS Office applications) • AnyConnect Web launch • Citrix Receiver, XenDesktop, and Xenon • Other non-browser-based and browser plugin-based applications <p>We introduced the following command: http-only-cookie.</p> <p><i>This feature is also in 9.2(3).</i></p>

Feature	Description
Virtual desktop access control using security group tagging	<p>The ASA now supports security group tagging-based policy control for Clientless SSL remote access to internal applications and websites. This feature uses Citrix's virtual desktop infrastructure (VDI) with XenDesktop as the delivery controller and the ASA's content transformation engine.</p> <p>See the following Citrix product documentation for more information:</p> <ul style="list-style-type: none"> • Policies for XenDesktop and XenApp: http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html • Managing policies in XenDesktop 7: http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-wrapper-rho.html • Using group policy editor for XenDesktop 7 policies: http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-use-gpms.html
OWA 2013 feature support has been added for Clientless SSL VPN	<p>Clientless SSL VPN supports the new features in OWA 2013 except for the following:</p> <ul style="list-style-type: none"> • Support for tablets and smartphones • Offline mode • Active Directory Federation Services (AD FS) 2.0. The ASA and AD FS 2.0 can't negotiate encryption protocols. <p>We did not modify any commands.</p>
Citrix XenDesktop 7.5 and StoreFront 2.5 support has been added for Clientless SSL VPN	<p>Clientless SSL VPN supports the access of XenDesktop 7.5 and StoreFront 2.5.</p> <p>See http://support.citrix.com/proddocs/topic/xenapp-xendesktop-75/cds-75-about-whats-new.html for the full list of XenDesktop 7.5 features, and for more details.</p> <p>See http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-about.html for the full list of StoreFront 2.5 features, and for more details.</p> <p>We did not modify any commands.</p>
Periodic certificate authentication	<p>When you enable periodic certificate authentication, the ASA stores certificate chains received from VPN clients and re-authenticates them periodically.</p> <p>We introduced or modified the following commands: periodic-authentication certificate, revocation-check, show vpn-sessiondb</p>
Certificate expiration alerts	<p>The ASA checks all CA and ID certificates in the trust points for expiration once every 24 hours. If a certificate is nearing expiration, a syslog will be issued as an alert. You can configure the reminder and recurrence intervals. By default, reminders will start at 60 days prior to expiration and recur every 7 days.</p> <p>We introduced or modified the following commands: crypto ca alerts expiration</p>

Feature	Description
Enforcement of the basic constraints CA flag	<p>Certificates without the CA flag now cannot be installed on the ASA as CA certificates by default. The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate. You can configure the ASA to allow installation of these certificates if desired.</p> <p>We introduced the following command: ca-check</p>
IKEv2 invalid selectors notification configuration	<p>Currently, if the ASA receives an inbound packet on an SA, and the packet's header fields are not consistent with the selectors for the SA, then the ASA discards the packet. You can now enable or disable sending an IKEv2 notification to the peer. Sending this notification is disabled by default.</p> <p>Note This feature is supported with AnyConnect 3.1.06060 and later.</p> <p>We introduced the following command: crypto ikev2 notify invalid-selectors</p>
IKEv2 pre-shared key in Hex	<p>You can now configure the IKEv2 pre-shared keys in hex.</p> <p>We introduced the following command: ikev2 local-authentication pre-shared-key hex, ikev2 remote-authentication pre-shared-key hex</p>
Administrative Features	
ASDM management authorization	<p>You can now configure management authorization separately for HTTP access vs. Telnet and SSH access.</p> <p>We introduced the following command: aaa authorization http console</p>
ASDM Username From Certificate Configuration	<p>When you enable ASDM certificate authentication (http authentication-certificate), you can configure how ASDM extracts the username from the certificate; you can also enable pre-filling the username at the login prompt.</p> <p>We introduced the following command: http username-from-certificate</p>
terminal interactive command to enable or disable help when you enter ? at the CLI	<p>Normally, when you enter ? at the ASA CLI, you see command help. To be able to enter ? as text within a command (for example, to include a ? as part of a URL), you can disable interactive help using the no terminal interactive command.</p> <p>We introduced the following command: terminal interactive</p>
REST API Features	
REST API Version 1.1	We added support for the REST API Version 1.1.
Support for token-based authentication (in addition to existing basic authentication)	Client can send log-in request to a specific URL; if successful, a token is returned (in response header). Client then uses this token (in a special request header) for sending additional API calls. The token is valid until explicitly invalidated, or the idle/session timeout is reached.

Feature	Description
Limited multiple-context support	<p>The REST API agent can now be enabled in multi-context mode; the CLI commands can be issued only in system-context mode (same commands as single-context mode).</p> <p>Pass-through CLI API commands can be used to configure any context, as follows.</p> <pre>https://<asa_admin_context_ip>/api/cli?context=<context_name></pre> <p>If the context parameter is not present, it is assumed that the request is directed to the admin context.</p>
Advanced (granular) inspection	<p>Granular inspection of these protocols is supported:</p> <ul style="list-style-type: none"> • DNS over UDP • HTTP • ICMP • ICMP ERROR • RTSP • SIP • FTP • DCERPC • IP Options • NetBIOS Name Server over IP • SQL*Net

Upgrade the Software

This section provides the upgrade path information and a link to complete your upgrade.

ASA Upgrade Path

To view your current version and model, use one of the following methods:

- CLI—Use the **show version** command.
- ASDM—Choose **Home > Device Dashboard > Device Information**.

See the following table for the upgrade path for your version. Some older versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.

Current Version	Interim Upgrade Version	Target Version
9.3(x)	—	Any of the following: → 9.4(x) → 9.3(x)
9.2(x)	—	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x)
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), or 9.1(7.4)	—	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
9.0(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.6(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.5(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.4(5+)	—	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.4(1) through 8.4(4)	Any of the following: → 9.0(2), 9.0(3), or 9.0(4) → 8.4(6)	→ 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.3(x)	→ 8.4(6)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.2(x) and earlier	→ 8.4(6)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Upgrade Link

To complete your upgrade, see the [ASA upgrade guide](#).

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.



Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can [register for an account](#). If you do not have a Cisco support contract, you can only look up bugs by ID; you cannot run searches.

For more information about the Cisco Bug Search Tool, see the [Bug Search Tool Help & FAQ](#).

Open Bugs in Version 9.4(x)

If you have a Cisco support contract, use the following dynamic search for all open bugs severity 3 and higher for Version 9.4(x):

- [9.4 open bug search](#).

The following table lists open bugs at the time of this Release Note publication.

Identifier	Description
CSCuo91169	Failover synchronization errors upon bulk synchronization operations
CSCuu90811	TLS CTP does not work in TLSv1.2 when GCM ciphers are used
CSCuv32879	Duplicate crypto ACE above an existing may cause traffic blackholing
CSCuv38775	"mac-address auto" command is not enabled by default
CSCuv61791	CWS redirection on ASA may corrupt sequence numbers with https traffic
CSCuv86562	Traceback: ASA crash in thread name fover_health_monitoring_thread
CSCuw10189	Alpha:Getting: LU allocate connection failed syslog on standby

Identifier	Description
CSCuw83618	ASA5508X SSD LED always green even when SSD is removed
CSCuw95262	After some time flash operations fail and configuration can not be saved
CSCux62229	ASA: IPSEC failover not encrypting IP Protocol 8 packets after failover
CSCux85525	XMLSoft libxml2 Encoding Conversion Denial of Service Vulnerability
CSCux85527	XMLSoft libxml2 xmlParserInputGrow Function Denial of Service Vulnerab
CSCux85528	XMLSoft libxml2 XML Entity Processing Denial of Service Vulnerability
CSCux85532	XMLSoft libxml2 xmlNextChar Function Memory Corruption Vulnerability
CSCux85533	XMLSoft libxml2 xmlParseXMLDecl Function Denial of Service Vulnerabili
CSCuy48237	Clientless SSL VPN CIFS stress test: ramfs_webvpn_file_open traceback
CSCuy71469	ASA : inspect ipsec-pass-thru not working after upgrade
CSCuy77638	Traceback while deleting an ACL element
CSCuy79179	Authentication failing after 9.4.2.11 upgrade.
CSCuy85511	libxml2 htmlParseNameComplex() Function Denial of Service Vulnerabilit
CSCuy90050	Page fault in DATAPATH thread, rip snp_fp
CSCuy99005	ASA: OSPF neighborhood failing on the Management Interface
CSCuz04534	Memory leak in 112 byte bin when packet hits PBR and WCCP rules
CSCuz05856	XMLSoft libxml2 xmlStringGetNodeList Function Memory Exhaustion Denial
CSCuz08625	ASA traceback in SSH thread
CSCuz11110	Share license server shows -939704796 local usage after upgrade
CSCuz14600	Kenton 9.5.1'boot system/boot config' commands not retained after reload
CSCuz20387	ASA : Traceback in Thread name: Session manager
CSCuz21178	ASA traceback in threadname ssh
CSCuz48749	ASA 5506 product power up issue if connected to 100M full duplex partner
CSCuz61092	Interface health-check failover causes OSPF not to advertise ASA as ABR
CSCuz80281	IPv6 neighbor discovery packet processing behavior
CSCuz90648	ASA/SFR Data Plane Down (2048 block exhaustion)
CSCuz91246	TCP conn count shows as negative - MPF policy blocks ALL TCP requests
CSCuz94862	IKEv2: Data rekey collisions can cause inactive IPsec SAs to get stuck

Identifier	Description
CSCuz98704	Crash in CP Processing thread after upgrade
CSCva00190	ASA 9.4.2.6 High CPU due to CTM message handler
CSCva02121	Traceback Thread Name: ci/console : debug menu ctm 103 crashes the ASA
CSCva02655	ASA sends invalid interface id to SFR for clientless VPN traffic
CSCva02817	ASA not rate limiting with DSCP bit set from the Server
CSCva04476	ASA crashing with thread name: DATAPATH-0-1903.
CSCva08992	Secondary ASA not sending PIM register message to RP
CSCva11419	ASA block 1550 depletion
CSCva16471	IPv6 OSPF routes do not update when a lower metric route is advertised

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 9.4(4.5)

The following table lists select resolved bugs at the time of this Release Note publication.

Caveat ID Number	Description
CSCtw90511	Packet captures cause CPU spike on Multi-Core platforms due to spin_lock
CSCuh89500	ASA: ifSpeed/ifHighSpeed not populated by SNMP for port-channel
CSCuj69650	ASA block new conns with "logging permit-hostdown" & TCP syslog is down
CSCum74032	ASA traceback on standby when SNMP polling
CSCum28756	ASA: Auth failures for SNMPv3 polling after unit rejoins cluster
CSCun16158	Cisco ASA Software IPsec Denial of Service Vulnerability
CSCum74032	ASA traceback on standby when SNMP polling
CSCup37416	Stale VPN Context entries cause ASA to stop encrypting traffic
CSCun16158	Cisco ASA Software IPsec Denial of Service Vulnerability
CSCup96099	"show resource usage detail counter all 1" causes cpu hog
CSCup37416	Stale VPN Context entries cause ASA to stop encrypting traffic
CSCuq80704	ASA classifies TCP packets as PAWS failure incorrectly
CSCup96099	"show resource usage detail counter all 1" causes cpu hog

Caveat ID Number	Description
CSCus29600	dhcprelay interface doesn't change by changing route
CSCuq80704	ASA classifies TCP packets as PAWS failure incorrectly
CSCus37458	ASA traceback in Thread name DATAPATH when handling multicast packet
CSCus29600	dhcprelay interface doesn't change by changing route
CSCut07712	ASA - TO the box traffic break due to int. missing in asp table routing
CSCus37458	ASA traceback in Thread name DATAPATH when handling multicast packet
CSCuu50708	ASA Traceback on 9.1.5.19
CSCut07712	ASA - TO the box traffic break due to int. missing in asp table routing
CSCuv61791	CWS redirection on ASA may corrupt sequence numbers with https traffic
CSCuu50708	ASA Traceback on 9.1.5.19
CSCuw04624	AVT : Missing HTTP Strict-Transport-Security Header in ASA 9.5.2
CSCuv61791	CWS redirection on ASA may corrupt sequence numbers with https traffic
CSCuw58948	An assertion was seen on the stby ASA after config sync
CSCuw04624	AVT : Missing HTTP Strict-Transport-Security Header in ASA 9.5.2
CSCuw71147	Traceback in Unicorn Proxy Thread, in http_header_by_name
CSCuw58948	An assertion was seen on the stby ASA after config sync
CSCuw88759	ASA: Protocol and Status showing UP without connecting the interface
CSCuw71147	Traceback in Unicorn Proxy Thread, in http_header_by_name
CSCuw95262	After some time flash operations fail and configuration can not be saved
CSCuw88759	ASA: Protocol and Status showing UP without connecting the interface
CSCux10499	Smart Tunnel starts and Java closes without any message
CSCuw95262	After some time flash operations fail and configuration can not be saved
CSCux17527	ASA memory leak related to Botnet
CSCux10499	Smart Tunnel starts and Java closes without any message
CSCux92157	ASA Traceback Assert in Thread Name: ssh_init with component ssh
CSCux17527	ASA memory leak related to Botnet
CSCux98029	ASA reloads with traceback in thread name DATAPATH or CP Processing
CSCux92157	ASA Traceback Assert in Thread Name: ssh_init with component ssh

Caveat ID Number	Description
CSCuy00296	Traceback in Thread: IPsec message handler
CSCux98029	ASA reloads with traceback in thread name DATAPATH or CP Processing
CSCuy06125	Re-adding context creates context without configs on some slaves
CSCuy00296	Traceback in Thread: IPsec message handler
CSCuy10665	HA: Number of interfaces mismatch after SFR module reload on both units
CSCuy06125	Re-adding context creates context without configs on some slaves
CSCuy15798	Add support for IPv6 assigned address field in Radius Accounting packet
CSCuy10665	HA: Number of interfaces mismatch after SFR module reload on both units
CSCuy22155	ASA generates unexpected syslog messages with mcast routing disabled
CSCuy15798	Add support for IPv6 assigned address field in Radius Accounting packet
CSCuy25163	Cisco ASA ACL ICMP Echo Request Code Filtering Vulnerability
CSCuy22155	ASA generates unexpected syslog messages with mcast routing disabled
CSCuy40207	Traceback: assertion "0" failed: file "ctm_daemon.c"
CSCuy25163	Cisco ASA ACL ICMP Echo Request Code Filtering Vulnerability
CSCuy43438	L2TP over IPsec can not be connected after disconnection from client.
CSCuy40207	Traceback: assertion "0" failed: file "ctm_daemon.c"
CSCuy47545	http config missing in multicontext after reload of stdby 916.9 or later
CSCuy43438	L2TP over IPsec can not be connected after disconnection from client.
CSCuy49291	Number of routes in the active and standby units are not same
CSCuy47545	http config missing in multicontext after reload of stdby 916.9 or later
CSCuy53516	ASA corrupts data in TLS-Proxy with TLS version 1.2
CSCuy49291	Number of routes in the active and standby units are not same
CSCuy54567	Evaluation of pix-asa for OpenSSL March 2016
CSCuy53516	ASA corrupts data in TLS-Proxy with TLS version 1.2
CSCuy55468	Unicorn Proxy Thread causing CP contention
CSCuy54567	Evaluation of pix-asa for OpenSSL March 2016
CSCuy58084	Unable to configure a user for ssh public auth only (tied w/ CSCuw90580)
CSCuy55468	Unicorn Proxy Thread causing CP contention

Caveat ID Number	Description
CSCuy63642	ASA 9.1(6) traceback processing outbound DTLS Packet
CSCuy58084	Unable to configure a user for ssh public auth only (tied w/ CSCuw90580)
CSCuy67333	SIP call transfer fail due to differences b/w fixing CallId and Refer-To
CSCuy63642	ASA 9.1(6) traceback processing outbound DTLS Packet
CSCuy74593	ASA AnyConnect IKEv2 scripts help customisations not served after reload
CSCuy67333	SIP call transfer fail due to differences b/w fixing CallId and Refer-To
CSCuy87597	ASA - Traceback in CP Processing Thread During Private Key Decryption
CSCuy74593	ASA AnyConnect IKEv2 scripts help customisations not served after reload
CSCuy89288	AnyConnect DTLS on-demand DPDs are not sent intermittently
CSCuy87597	ASA - Traceback in CP Processing Thread During Private Key Decryption
CSCuy89425	AAA: RSA/SDI unable to set new PIN
CSCuy89288	AnyConnect DTLS on-demand DPDs are not sent intermittently
CSCuy91405	ASA should not load-balance same flow traffic over port-channel CCL
CSCuy89425	AAA: RSA/SDI unable to set new PIN
CSCuy98769	Slow ASA OSPF interface transition from DOWN to WAITING after failover
CSCuy91405	ASA should not load-balance same flow traffic over port-channel CCL
CSCuz00075	ASA 9.4.1.5 - Incorrect memory usage reported in 'show mem det'
CSCuy98769	Slow ASA OSPF interface transition from DOWN to WAITING after failover
CSCuz00077	ASA 9.1.6.4 traceback with Thread Name: telnet/ci
CSCuz00075	ASA 9.4.1.5 - Incorrect memory usage reported in 'show mem det'
CSCuz04385	IPSec rekey collision handling failure cases IKE tunnel drop
CSCuz00077	ASA 9.1.6.4 traceback with Thread Name: telnet/ci
CSCuz04534	Memory leak in 112 byte bin when packet hits PBR and WCCP rules
CSCuz04385	IPSec rekey collision handling failure cases IKE tunnel drop
CSCuz06125	Active and Standby ASA use same MAC addr with only active MAC configured
CSCuz04534	Memory leak in 112 byte bin when packet hits PBR and WCCP rules
CSCuz06153	Incorrect msg shown when configuring MAC addr same as already configured
CSCuz06125	Active and Standby ASA use same MAC addr with only active MAC configured

Caveat ID Number	Description
CSCuz06499	WebVPN: Webpage not fully rewritten when ASA has the same FQDN as srv
CSCuz06153	Incorrect msg shown when configuring MAC addr same as already configured
CSCuz08625	ASA traceback in SSH thread
CSCuz06499	WebVPN: Webpage not fully rewritten when ASA has the same FQDN as srv
CSCuz09255	ASA does not respond to NS in Active/Active HA
CSCuz08625	ASA traceback in SSH thread
CSCuz09255	ASA does not respond to NS in Active/Active HA
CSCuz09394	infinite loop in JS rewriter state machine when return followed by var
CSCuz09394	infinite loop in JS rewriter state machine when return followed by var
CSCuz11685	Cisco ASA Software Internet Key Exchange Version 1 XAUTH Denial of Service Vulnerability
CSCuz11685	Cisco ASA Software Internet Key Exchange Version 1 XAUTH Denial of Service Vulnerability
CSCuz14600	Kenton 9.5.1 'boot system/boot config' commands not retained after reload
CSCuz14600	Kenton 9.5.1 'boot system/boot config' commands not retained after reload
CSCuz14808	5585-10 traceback in Thread Name: idfw_proc
CSCuz14808	5585-10 traceback in Thread Name: idfw_proc
CSCuz16398	Incorrect modification of NAT divert table.
CSCuz16398	Incorrect modification of NAT divert table.
CSCuz16565	9.6.2 EST - assertion "0" failed: file "snp_vxlan.c"
CSCuz16565	9.6.2 EST - assertion "0" failed: file "snp_vxlan.c"
CSCuz21178	ASA traceback in threadname ssh
CSCuz21178	ASA traceback in threadname ssh
CSCuz27165	BTF is not blocking blacklisted domain with more than 2 labels in it
CSCuz27165	BTF is not blocking blacklisted domain with more than 2 labels in it
CSCuz28000	Context config may get rejected if all the units in Cluster reloaded
CSCuz28000	Context config may get rejected if all the units in Cluster reloaded
CSCuz30425	Network command disappears from BGP after reload with name
CSCuz30425	Network command disappears from BGP after reload with name

Caveat ID Number	Description
CSCuz33255	Traceback in IKEv2 Daemon with 20+ second CPU hog.
CSCuz33255	Traceback in IKEv2 Daemon with 20+ second CPU hog.
CSCuz36545	Drop down menu doesn't work on Simfosa web page
CSCuz36545	Drop down menu doesn't work on Simfosa web page
CSCuz36938	Traceback on editing a network object on exceeding the max snmp hosts
CSCuz36938	Traceback on editing a network object on exceeding the max snmp hosts
CSCuz38115	ASA Tback when large ACL applied to interface with object-group-search
CSCuz38115	ASA Tback when large ACL applied to interface with object-group-search
CSCuz38180	ASA: Page Fault traceback in DATAPATH on standby ASA after booting up
CSCuz38180	ASA: Page Fault traceback in DATAPATH on standby ASA after booting up
CSCuz38703	ASA capture type isakmp saving malformed ISAKMP packets
CSCuz38703	ASA capture type isakmp saving malformed ISAKMP packets
CSCuz38888	WebVPN rewrite fails for MSCA Cert enrollment page / VBScript
CSCuz38888	WebVPN rewrite fails for MSCA Cert enrollment page / VBScript
CSCuz40081	ASA memory leak due to vpnfo
CSCuz40081	ASA memory leak due to vpnfo
CSCuz40793	Interfaces get deleted on SFR during HA configuration sync
CSCuz40793	Interfaces get deleted on SFR during HA configuration sync
CSCuz41033	dynamic crypto map fails if named the same as static crypto map
CSCuz41033	dynamic crypto map fails if named the same as static crypto map
CSCuz42390	ASA Stateful failover for DRP works intermittently
CSCuz42390	ASA Stateful failover for DRP works intermittently
CSCuz44968	Commands not installed on Standby due to parser switch
CSCuz44968	Commands not installed on Standby due to parser switch
CSCuz52474	Evaluation of pix-asa for OpenSSL May 2016
CSCuz52474	Evaluation of pix-asa for OpenSSL May 2016
CSCuz54193	ASA: Traceback on ASA in Datapath as we enable SFR traffic redirection
CSCuz54193	ASA: Traceback on ASA in Datapath as we enable SFR traffic redirection

Caveat ID Number	Description
CSCuz54545	ASA Address not mapped traceback - configuring snmp-server host
CSCuz54545	ASA Address not mapped traceback - configuring snmp-server host
CSCuz58142	ASA Access-list missing and losing elements Warning Message enhancement
CSCuz58142	ASA Access-list missing and losing elements Warning Message enhancement
CSCuz60555	ASA-2-321006 May be received invalidly when memory is not high
CSCuz60555	ASA-2-321006 May be received invalidly when memory is not high
CSCuz61092	Interface health-check failover causes OSPF not to advertise ASA as ABR
CSCuz61092	Interface health-check failover causes OSPF not to advertise ASA as ABR
CSCuz63531	Observing Memory corruption, assert for debug ospf
CSCuz63531	Observing Memory corruption, assert for debug ospf
CSCuz66269	SCP Client not allow to enter password with "no ssh stricthostkeycheck"
CSCuz66269	SCP Client not allow to enter password with "no ssh stricthostkeycheck"
CSCuz66661	ASA Cut-through Proxy inactivity timeout not working
CSCuz66661	ASA Cut-through Proxy inactivity timeout not working
CSCuz67349	ASA Cluster fragments reassembled before transmission with no inspection
CSCuz67349	ASA Cluster fragments reassembled before transmission with no inspection
CSCuz67590	ASA may Traceback with Thread Name: cluster rx thread
CSCuz67590	ASA may Traceback with Thread Name: cluster rx thread
CSCuz67596	ASA may Traceback with Thread Name: Unicorn Admin Handler
CSCuz67596	ASA may Traceback with Thread Name: Unicorn Admin Handler
CSCuz67690	ASA crashed due to Election severe problem no master is promoted
CSCuz67690	ASA crashed due to Election severe problem no master is promoted
CSCuz70330	ASA: SSH being denied on the ASA device as the maximum limit is reached
CSCuz70330	ASA: SSH being denied on the ASA device as the maximum limit is reached
CSCuz72352	traceback during tls-proxy handshake
CSCuz72352	traceback during tls-proxy handshake
CSCuz77293	OSPF multicast filter rules missing in cluster slave
CSCuz77293	OSPF multicast filter rules missing in cluster slave

Caveat ID Number	Description
CSCuz77818	PIM BiDir DF Elections stuck in "offer" state on some interfaces
CSCuz77818	PIM BiDir DF Elections stuck in "offer" state on some interfaces
CSCuz79800	ASA cant delete ACL lines and remarks - Specified remark does not exist
CSCuz79800	ASA cant delete ACL lines and remarks - Specified remark does not exist
CSCuz80281	IPv6 neighbor discovery packet processing behavior
CSCuz80281	IPv6 neighbor discovery packet processing behavior
CSCuz87146	nat-t-disable feature is not working for ikev2
CSCuz87146	nat-t-disable feature is not working for ikev2
CSCuz89989	Ikev1 tunnel drops with reason " Peer Address Changed"
CSCuz89989	Ikev1 tunnel drops with reason " Peer Address Changed"
CSCuz90648	2048/1550/9344 Byte block leak cause traffic disruption & module failure
CSCuz90648	2048/1550/9344 Byte block leak cause traffic disruption & module failure
CSCuz92074	ASA with PAT fails to untranslate SIP Via field that doesnt contain port
CSCuz92074	ASA with PAT fails to untranslate SIP Via field that doesnt contain port
CSCuz92921	ASA crashes while clearing global access-list
CSCuz92921	ASA crashes while clearing global access-list
CSCuz93626	Inspect-mmp configuration is missing in latest branches.
CSCuz93626	Inspect-mmp configuration is missing in latest branches.
CSCuz94158	Hash miscalculation for "Any" address on inside
CSCuz94158	Hash miscalculation for "Any" address on inside
CSCuz94862	IKEv2: Data rekey collisions can cause inactive IPsec SAs to get stuck
CSCuz94862	IKEv2: Data rekey collisions can cause inactive IPsec SAs to get stuck
CSCuz95806	DNS Doctoring DNS64 is not working
CSCuz95806	DNS Doctoring DNS64 is not working
CSCuz98220	ASA traceback with Thread Name: Dispatch Unit
CSCuz98220	ASA traceback with Thread Name: Dispatch Unit
CSCuz98704	Traceback in CP Processing thread after upgrade
CSCuz98704	Traceback in CP Processing thread after upgrade

Caveat ID Number	Description
CSCva00190	ASA 9.4.2.6 High CPU due to CTM message handler due to chip resets
CSCva00190	ASA 9.4.2.6 High CPU due to CTM message handler due to chip resets
CSCva00939	Remove ACL warning messages in show access-list when FQDN is resolved
CSCva00939	Remove ACL warning messages in show access-list when FQDN is resolved
CSCva01570	Unexpected end of file logon.html in WebVPN
CSCva01570	Unexpected end of file logon.html in WebVPN
CSCva02655	ASA sends invalid interface id to SFR for clientless VPN traffic
CSCva02655	ASA sends invalid interface id to SFR for clientless VPN traffic
CSCva02817	ASA not rate limiting with DSCP bit set from the Server
CSCva02817	ASA not rate limiting with DSCP bit set from the Server
CSCva03607	show service-policy output reporting incorrect values
CSCva03607	show service-policy output reporting incorrect values
CSCva05513	ASA: SLA Monitor not working with floating timeout configured to nonzero
CSCva05513	ASA: SLA Monitor not working with floating timeout configured to nonzero
CSCva07268	Unable to auth a 2nd time via clientless after ASA upgrade
CSCva07268	Unable to auth a 2nd time via clientless after ASA upgrade
CSCva12520	snmpwalk not working for some NAT OIDs
CSCva12520	snmpwalk not working for some NAT OIDs
CSCva15911	On reloading the ASA, ASA mounts SSD as disk 0, instead of the flash.
CSCva15911	On reloading the ASA, ASA mounts SSD as disk 0, instead of the flash.
CSCva16471	IPv6 OSPF routes do not update when a lower metric route is advertised
CSCva16471	IPv6 OSPF routes do not update when a lower metric route is advertised
CSCva22048	ASA: SIP Call Drops with PAT when same media port used in multiple calls
CSCva22048	ASA: SIP Call Drops with PAT when same media port used in multiple calls
CSCva24799	TLS Proxy feature missing client trust-point command
CSCva24799	TLS Proxy feature missing client trust-point command
CSCva31378	ASA traceback at Thread Name: rtcli async executor process
CSCva31378	ASA traceback at Thread Name: rtcli async executor process

Caveat ID Number	Description
CSCva35439	ASA DATAPATH traceback (Cluster)
CSCva35439	ASA DATAPATH traceback (Cluster)
CSCva35990	Traceback on CP Process with H323 inspection, rip h323_service_early_msg
CSCva35990	Traceback on CP Process with H323 inspection, rip h323_service_early_msg
CSCva36202	BGP Socket not open in ASA after reload
CSCva36202	BGP Socket not open in ASA after reload
CSCva36884	Cisco ASA Cross Site Scripting SSLVPN Vulnerability
CSCva36884	Cisco ASA Cross Site Scripting SSLVPN Vulnerability
CSCva38556	Cisco ASA Input Validation File Injection Vulnerability
CSCva38556	Cisco ASA Input Validation File Injection Vulnerability
CSCva39094	ASA traceback in CLI thread while making MPF changes
CSCva39094	ASA traceback in CLI thread while making MPF changes
CSCva39804	Interfaces get deleted on SFR during cluster rejoining
CSCva39804	Interfaces get deleted on SFR during cluster rejoining
CSCva40844	Crypto accelerator ring timeout causes packet drops
CSCva40844	Crypto accelerator ring timeout causes packet drops
CSCva43746	ASA 'show inventory' shows 'Driver Error, invalid query ready'
CSCva43746	ASA 'show inventory' shows 'Driver Error, invalid query ready'
CSCva45590	ASA OSPFv3 interface ID changes upon disabling/enabling failover
CSCva45590	ASA OSPFv3 interface ID changes upon disabling/enabling failover
CSCva46920	Traceback in Thread Name: ssh when issuing show tls-proxy session detail
CSCva46920	Traceback in Thread Name: ssh when issuing show tls-proxy session detail
CSCva47608	SCTP MH:pin hole removed and added freq on standby with dual nat
CSCva47608	SCTP MH:pin hole removed and added freq on standby with dual nat
CSCva49256	memory leak in ssh
CSCva49256	memory leak in ssh
CSCva50554	ASA uses ":::" for host IP addresses if booted with an improper config
CSCva50554	ASA uses ":::" for host IP addresses if booted with an improper config

Caveat ID Number	Description
CSCva53581	Increasing the global ARP request pool
CSCva53581	Increasing the global ARP request pool
CSCva56343	Clustering: TFW asynchronous flow packet drop due to L2 entry timeout
CSCva56343	Clustering: TFW asynchronous flow packet drop due to L2 entry timeout
CSCva62667	Shut down interfaces shows up in ASP routing table
CSCva62667	Shut down interfaces shows up in ASP routing table
CSCva68364	SNMPv3 active engineID is not reset when ASA is replaced
CSCva68364	SNMPv3 active engineID is not reset when ASA is replaced
CSCva68987	ASA drops ICMP request packets when ICMP inspection is disabled
CSCva68987	ASA drops ICMP request packets when ICMP inspection is disabled
CSCva69346	Unable to relay DHCP discover packet from ASA when NAT is matched
CSCva69346	Unable to relay DHCP discover packet from ASA when NAT is matched
CSCva69584	OSPF generates Type-5 LSA with incorrect mask, which gets stuck in LSDB
CSCva69584	OSPF generates Type-5 LSA with incorrect mask, which gets stuck in LSDB
CSCva69799	ASA stuck in boot loop due to FIPS Self-Test failure
CSCva69799	ASA stuck in boot loop due to FIPS Self-Test failure
CSCva70095	ASA negotiates TLS1.2 when server in tls-proxy
CSCva70095	ASA negotiates TLS1.2 when server in tls-proxy
CSCva71783	ICMP error packets in response to reply packets are dropped
CSCva71783	ICMP error packets in response to reply packets are dropped
CSCva76568	ASA : Enabling IKEv1/IKEv2 opens RADIUS ports
CSCva76568	ASA : Enabling IKEv1/IKEv2 opens RADIUS ports
CSCva77852	ipsecvpn-ikev2_oth: 5525 9.4.2.11 traceback in Thread Name: IKEv2 Daemon
CSCva77852	ipsecvpn-ikev2_oth: 5525 9.4.2.11 traceback in Thread Name: IKEv2 Daemon
CSCva81412	ASR9000 BGP Graceful Restart doesnt work as expected
CSCva81412	ASR9000 BGP Graceful Restart doesnt work as expected
CSCva81749	IPV6 address not assigned when connecting via IPSEC protocol
CSCva81749	IPV6 address not assigned when connecting via IPSEC protocol

Caveat ID Number	Description
CSCva84635	ASA: CHILD_SA collision brings down IKEv2 SA
CSCva84635	ASA: CHILD_SA collision brings down IKEv2 SA
CSCva85382	ASA memory leak for CTS SGT mappings
CSCva85382	ASA memory leak for CTS SGT mappings
CSCva86626	HTML5: Guacamole server requires page refresh
CSCva86626	HTML5: Guacamole server requires page refresh
CSCva87160	OTP authentication is not working for clientless ssl vpn
CSCva87160	OTP authentication is not working for clientless ssl vpn
CSCva88796	AnyConnect Sessions Cannot Connect Due to Stuck L2TP Uauth Sessions
CSCva88796	AnyConnect Sessions Cannot Connect Due to Stuck L2TP Uauth Sessions
CSCva90419	issuer-name falsely detecting duplicates in certificate map using attr
CSCva90419	issuer-name falsely detecting duplicates in certificate map using attr
CSCva90806	ASA Traceback when issue 'show asp table classify domain permit'
CSCva90806	ASA Traceback when issue 'show asp table classify domain permit'
CSCva91420	ASA Traceback in CTM Message Handler
CSCva91420	ASA Traceback in CTM Message Handler
CSCva92151	Cisco ASA SNMP Remote Code Execution Vulnerability
CSCva92151	Cisco ASA SNMP Remote Code Execution Vulnerability
CSCva92813	ASA Cluster DHCP Relay doesn't forward the server replies to the client
CSCva92813	ASA Cluster DHCP Relay doesn't forward the server replies to the client
CSCva92975	ASA 5585-60 dropping out of cluster with traceback
CSCva92975	ASA 5585-60 dropping out of cluster with traceback
CSCva94702	Enqueue failures on DP-CP queue may stall inspected TCP connection
CSCva94702	Enqueue failures on DP-CP queue may stall inspected TCP connection
CSCva97863	971 EST - Console hang on show capture
CSCva97863	971 EST - Console hang on show capture
CSCva98240	SIP: Address from Route: header not translated correctly
CSCva98240	SIP: Address from Route: header not translated correctly

Caveat ID Number	Description
CSCvb03994	Traceback in IKE_DBG
CSCvb03994	Traceback in IKE_DBG
CSCvb04685	Unable to delete the SNMP config
CSCvb04685	Unable to delete the SNMP config
CSCvb05667	H.323 inspection causes Traceback in Thread Name: CP Processing
CSCvb05667	H.323 inspection causes Traceback in Thread Name: CP Processing
CSCvb05787	traceback in network udpmod_get after anyconnect test load application
CSCvb05787	traceback in network udpmod_get after anyconnect test load application
CSCvb13737	wr mem/ wr standby is not syncing configs on standby
CSCvb13737	wr mem/ wr standby is not syncing configs on standby
CSCvb14997	ASA DHCP Relay rewrites netmask and gw received as part of DHCP Offer
CSCvb14997	ASA DHCP Relay rewrites netmask and gw received as part of DHCP Offer
CSCvb15265	ASA Page fault traceback in Thread Name: DATAPATH
CSCvb15265	ASA Page fault traceback in Thread Name: DATAPATH
CSCvb19251	ASA as DHCP relay drops DHCP 150 Inform message
CSCvb19251	ASA as DHCP relay drops DHCP 150 Inform message
CSCvb19843	Buffer Overflow in ASA Leads to Remote Code Execution
CSCvb19843	Buffer Overflow in ASA Leads to Remote Code Execution
CSCvb20256	Sweet32 Vulnerability in ASA's SSH Implementation
CSCvb20256	Sweet32 Vulnerability in ASA's SSH Implementation
CSCvb21922	Remove ACL warning messages in show access-list when FQDN is unresolved
CSCvb21922	Remove ACL warning messages in show access-list when FQDN is unresolved
CSCvb22435	ASA Traceback in thread name CP Processing due to DCERPC inspection
CSCvb22435	ASA Traceback in thread name CP Processing due to DCERPC inspection
CSCvb22848	ASA 9.1.7-9 crash in Thread Name: NIC status poll
CSCvb22848	ASA 9.1.7-9 crash in Thread Name: NIC status poll
CSCvb26119	Webvpn rewriter failing on matterport.com
CSCvb26119	Webvpn rewriter failing on matterport.com

Caveat ID Number	Description
CSCvb27868	ASA 1550 block depletion with multi-context transparent firewall
CSCvb27868	ASA 1550 block depletion with multi-context transparent firewall
CSCvb29688	Stale VPN Context entries cause ASA to stop encrypting traffic despite fix for CSCup37416
CSCvb29688	Stale VPN Context entries cause ASA to stop encrypting traffic despite fix for CSCup37416
CSCvb31055	ASA Multiple Context SNMP PAT Interface Missing
CSCvb31055	ASA Multiple Context SNMP PAT Interface Missing
CSCvb31833	Traceback : ASA with Threadname: DATAPATH-0-1790
CSCvb31833	Traceback : ASA with Threadname: DATAPATH-0-1790
CSCvb32297	WebVPN:VNC plugin:Java:Connection reset by peer: socket write error
CSCvb32297	WebVPN:VNC plugin:Java:Connection reset by peer: socket write error
CSCvb33009	Cisco ASA Signature Verification Misleading Digital Signing Text On Boot
CSCvb33009	Cisco ASA Signature Verification Misleading Digital Signing Text On Boot
CSCvb33013	Cisco ASA Remove Mis-leading Secure Boot commands on non-SB hardware
CSCvb33013	Cisco ASA Remove Mis-leading Secure Boot commands on non-SB hardware
CSCvb36199	Thread Name: snmp ASA5585-SSP-2 running 9.6.2 traceback
CSCvb36199	Thread Name: snmp ASA5585-SSP-2 running 9.6.2 traceback
CSCvb37456	Failover after IKE rekey fails to initiate ph1 rekey on act device
CSCvb37456	Failover after IKE rekey fails to initiate ph1 rekey on act device
CSCvb38522	ASA PKI OCSP failing - CRYPTO_PKI: failed to decode OCSP response data.
CSCvb38522	ASA PKI OCSP failing - CRYPTO_PKI: failed to decode OCSP response data.
CSCvb39147	Lower NFS throughput rate on Cisco ASA platform
CSCvb39147	Lower NFS throughput rate on Cisco ASA platform
CSCvb40847	ASA not sending Authen Session End log if user logs out manually
CSCvb40847	ASA not sending Authen Session End log if user logs out manually
CSCvb40898	Cisco ASA Software DNS Denial of Service Vulnerability
CSCvb40898	Cisco ASA Software DNS Denial of Service Vulnerability
CSCvb43120	ASA Traceback in Checkheaps Thread

Caveat ID Number	Description
CSCvb43120	ASA Traceback in Checkheaps Thread
CSCvb45039	ASA traceback with Thread Name aaa_shim_thread
CSCvb45039	ASA traceback with Thread Name aaa_shim_thread
CSCvb46321	Cisco ASA Software and Cisco FTD Software TCP Normalizer Denial of Service Vulnerability
CSCvb46321	Cisco ASA Software and Cisco FTD Software TCP Normalizer Denial of Service Vulnerability
CSCvb47006	ASA traceback observed on auto-update thread.
CSCvb47006	ASA traceback observed on auto-update thread.
CSCvb48640	Evaluation of pix-asa for Openssl September 2016
CSCvb48640	Evaluation of pix-asa for Openssl September 2016
CSCvb49273	Traceback triggered by CoA on ASA when sending/receiving to/from ISE
CSCvb49273	Traceback triggered by CoA on ASA when sending/receiving to/from ISE
CSCvb49445	IKEv2: It is NOT cleaning the sessions after disconnected from the client.
CSCvb49445	IKEv2: It is NOT cleaning the sessions after disconnected from the client.
CSCvb50301	ASA traceback at Thread Name: rtcli
CSCvb50301	ASA traceback at Thread Name: rtcli
CSCvb50609	RADIUS authorization request does not send Called-Station-ID attribute
CSCvb50609	RADIUS authorization request does not send Called-Station-ID attribute
CSCvb52157	viewer_dart.js file not loading correctly
CSCvb52157	viewer_dart.js file not loading correctly
CSCvb52988	ASA Traceback Thread Name: emweb/https
CSCvb52988	ASA Traceback Thread Name: emweb/https
CSCvb57817	EIGRP: Need to add large number error handling when getting scaled bandwidth
CSCvb57817	EIGRP: Need to add large number error handling when getting scaled bandwidth
CSCvb58087	Object-group-search redundant service group objects are incorrectly removed
CSCvb58087	Object-group-search redundant service group objects are incorrectly removed
CSCvb63503	AAA session handle leak with IKEv2 when denied due to time range
CSCvb63503	AAA session handle leak with IKEv2 when denied due to time range

Caveat ID Number	Description
CSCvb63819	ASA-SM traceback with Thread : fover_parse during upgrade OS 9.1.6 to 9.4.3
CSCvb63819	ASA-SM traceback with Thread : fover_parse during upgrade OS 9.1.6 to 9.4.3
CSCvb64161	ASA fairly infrequently rewrites the dest MAC address of multicast packet for client
CSCvb64161	ASA fairly infrequently rewrites the dest MAC address of multicast packet for client
CSCvb66593	webvpn_state cookie information disclosure in url
CSCvb66593	webvpn_state cookie information disclosure in url
CSCvb68766	ASA traceback at Thread Name: IKE Daemon.
CSCvb68766	ASA traceback at Thread Name: IKE Daemon.
CSCvb74249	ASA dropping traffic with TCP syslog configured in multicontext mode
CSCvb74249	ASA dropping traffic with TCP syslog configured in multicontext mode
CSCvb78614	4GE-SSM RJ45 interface may drop traffic due to interface "rate limit drops"
CSCvb78614	4GE-SSM RJ45 interface may drop traffic due to interface "rate limit drops"
CSCvb85624	Evaluation of pix-asa for CVE-2016-5195 (DIRTY CoW)
CSCvb85624	Evaluation of pix-asa for CVE-2016-5195 (DIRTY CoW)
CSCvb87586	Failed to ssh management interface after failover and plug-in/out
CSCvb87586	Failed to ssh management interface after failover and plug-in/out
CSCvb89988	WebVPN: Internal page login button not working through rewriter
CSCvb89988	WebVPN: Internal page login button not working through rewriter
CSCvb92125	ASA drops DNS PTR Reply with reason Label length exceeded during rewrite
CSCvb92125	ASA drops DNS PTR Reply with reason Label length exceeded during rewrite
CSCvb92548	ASA matches incorrect ACL with object-group-search enabled
CSCvb92548	ASA matches incorrect ACL with object-group-search enabled
CSCvb92823	ASA SIP inspection may delay transmission of 200 OK when embedded with NOTIFY
CSCvb92823	ASA SIP inspection may delay transmission of 200 OK when embedded with NOTIFY
CSCvc00689	ASA : memory leak due to ikev2
CSCvc00689	ASA : memory leak due to ikev2
CSCvc04741	ASA DHCP relay is incompatible with intercept-dhcp feature
CSCvc04741	ASA DHCP relay is incompatible with intercept-dhcp feature

Caveat ID Number	Description
CSCvc05005	ASA cluster TCP/SSL ports are not displayed on LISTEN state
CSCvc05005	ASA cluster TCP/SSL ports are not displayed on LISTEN state
CSCvc06150	ASA unable to add multiple attribute entries in a certificate map
CSCvc06150	ASA unable to add multiple attribute entries in a certificate map
CSCvc07330	ASAv may crash when running webvpn
CSCvc07330	ASAv may crash when running webvpn
CSCvc14190	ASA fails SSL VPN session establishment with EC under load
CSCvc14190	ASA fails SSL VPN session establishment with EC under load
CSCvc14448	9.6.2 - Traceback during AnyConnect IKEv2 Performance Test
CSCvc14448	9.6.2 - Traceback during AnyConnect IKEv2 Performance Test
CSCvc14502	ASA multicontext disallowing new conns with TCP syslog unreachable and logging permit-hostdown set
CSCvc14502	ASA multicontext disallowing new conns with TCP syslog unreachable and logging permit-hostdown set
CSCvc19318	ASA traceback at Thread Name: sch_syslog
CSCvc19318	ASA traceback at Thread Name: sch_syslog
CSCvc22193	DSCP Markings Not Copied to Outer IP Header With IPsec Encapsulation
CSCvc22193	DSCP Markings Not Copied to Outer IP Header With IPsec Encapsulation
CSCvc23838	Cisco ASA Heap Overflow in Webvpn CIFS
CSCvc23838	Cisco ASA Heap Overflow in Webvpn CIFS
CSCvc24380	Traceback on thread name IKE Daemon at mqc_enable_qos_for_tunnel
CSCvc24380	Traceback on thread name IKE Daemon at mqc_enable_qos_for_tunnel
CSCvc24657	MIB object compMemPoolHCUsed disappeared
CSCvc24657	MIB object compMemPoolHCUsed disappeared
CSCvc24788	ASA: OspfV3 routes are not getting installed
CSCvc24788	ASA: OspfV3 routes are not getting installed
CSCvc25281	Error synchronizing the SNMPv3 user after rebooting a cluster unit
CSCvc25281	Error synchronizing the SNMPv3 user after rebooting a cluster unit
CSCvc25409	ASA memory leak in CloneOctetString when using SNMP polling

Caveat ID Number	Description
CSCvc25409	ASA memory leak in CloneOctetString when using SNMP polling
CSCvc33796	Implement speed improvements for ACL and NAT table compilation
CSCvc33796	Implement speed improvements for ACL and NAT table compilation
CSCvc36535	ASA traceback in Thread Name: ssh, rip igb_disable_rx_queues after no shutdown of interface
CSCvc36535	ASA traceback in Thread Name: ssh, rip igb_disable_rx_queues after no shutdown of interface
CSCvc37557	SSL connection hangs between ASA and backend server in clientless WebVPN
CSCvc37557	SSL connection hangs between ASA and backend server in clientless WebVPN
CSCvc38425	ASA with FirePOWER module generates traceback and reloads or causes process not running
CSCvc38425	ASA with FirePOWER module generates traceback and reloads or causes process not running
CSCvc44240	ASA clustering: mac-address cmd is ignored on spanned port-channel interface in 9.6.2
CSCvc44240	ASA clustering: mac-address cmd is ignored on spanned port-channel interface in 9.6.2
CSCvc48640	ASA not update access-list dynamically when forward-reference enable is configured
CSCvc48640	ASA not update access-list dynamically when forward-reference enable is configured
CSCvc52072	Webvpn portal not displayed correctly for connections landing on default webvpn group.
CSCvc52072	Webvpn portal not displayed correctly for connections landing on default webvpn group.
CSCvc52272	ASA inspection-MPF ACL changes are not getting ordered correctly in the ASP Table
CSCvc52272	ASA inspection-MPF ACL changes are not getting ordered correctly in the ASP Table
CSCvc52504	ASA may traceback with Thread Name: Unicorn Admin Handler
CSCvc52504	ASA may traceback with Thread Name: Unicorn Admin Handler
CSCvc52879	Reloading Active unit in Active/Standby ASA failover pair is not triggering a failover.
CSCvc52879	Reloading Active unit in Active/Standby ASA failover pair is not triggering a failover.
CSCvc55674	ASA: IPSec SA failed to come up
CSCvc55674	ASA: IPSec SA failed to come up

Caveat ID Number	Description
CSCvc55974	ikev2 handles get leaked in a L2L setup
CSCvc55974	ikev2 handles get leaked in a L2L setup
CSCvc56526	CEP records edit page take minutes to load
CSCvc56526	CEP records edit page take minutes to load
CSCvc58272	ASA incorrectly processing negative numbers in wrappers, resulting in graphical webvpn issue
CSCvc58272	ASA incorrectly processing negative numbers in wrappers, resulting in graphical webvpn issue
CSCvc60254	SIP: 200 OK messages with multiple seqments not reassembled correctly
CSCvc60254	SIP: 200 OK messages with multiple seqments not reassembled correctly
CSCvc60964	ASA L3 Cluster: DHCP relay drops DHCPOFFER in case of asymmetric routing
CSCvc60964	ASA L3 Cluster: DHCP relay drops DHCPOFFER in case of asymmetric routing
CSCvc61818	CTP after failed attempt sends the domain along with the username
CSCvc61818	CTP after failed attempt sends the domain along with the username
CSCvc62252	Tracking route is up while the reachability is down
CSCvc62252	Tracking route is up while the reachability is down
CSCvc62556	Traceback in ASA Cluster Thread Name: qos_metric_daemon
CSCvc62556	Traceback in ASA Cluster Thread Name: qos_metric_daemon
CSCvc79371	ASA nat pool not getting updated correctly.
CSCvc79371	ASA nat pool not getting updated correctly.
CSCvc79454	Unable to configure ssh public auth for script users
CSCvc79454	Unable to configure ssh public auth for script users
CSCvc82146	ASA traceback in threadname Datapath
CSCvc82146	ASA traceback in threadname Datapath
CSCvc85369	ASA does not respond to IPv6 MLD Query.
CSCvc85369	ASA does not respond to IPv6 MLD Query.
CSCvc87914	ASA traceback and Reload on Config Sync Failure
CSCvc87914	ASA traceback and Reload on Config Sync Failure
CSCvc88411	1550-byte block depletion seen due to Radius Accounting packets

Caveat ID Number	Description
CSCvc88411	1550-byte block depletion seen due to Radius Accounting packets
CSCvc93947	ASA(9.1.7.12):Connection entries created for multicast streams through standby ASA.
CSCvc93947	ASA(9.1.7.12):Connection entries created for multicast streams through standby ASA.
CSCvd01736	L2TP connects only sometimes when DHCP used
CSCvd01736	L2TP connects only sometimes when DHCP used
CSCvd03343	Unable to configure SSH public key auth for non-system contexts
CSCvd03343	Unable to configure SSH public key auth for non-system contexts
CSCvd06022	ASA-FP9300 Crashed in thread name IPSEC MESSAGE HANDLER after upgrade
CSCvd06022	ASA-FP9300 Crashed in thread name IPSEC MESSAGE HANDLER after upgrade
CSCvd08200	Slow Memory leak in ASA
CSCvd08200	Slow Memory leak in ASA
CSCvd15843	Port Forwarding Session times out due to "vpn-idle-timeout" in group-policy while passing data
CSCvd15843	Port Forwarding Session times out due to "vpn-idle-timeout" in group-policy while passing data
CSCvd21154	5585 does not unbundle its data intfs for 30 seconds after leaving cluste
CSCvd21154	5585 does not unbundle its data intfs for 30 seconds after leaving cluste
CSCvd21541	Cannot delete port-object once created under the Service object group in ASA 944
CSCvd21541	Cannot delete port-object once created under the Service object group in ASA 944
CSCvd23016	ASA may traceback when copying capture out using tftp
CSCvd23016	ASA may traceback when copying capture out using tftp
CSCvd23471	ASA may traceback while loading a large context config during bootup
CSCvd23471	ASA may traceback while loading a large context config during bootup
CSCvd24066	ASA drops web traffic when IM inspection is enabled.
CSCvd24066	ASA drops web traffic when IM inspection is enabled.
CSCvd28859	ASA: PBR Memory leak for ICMP traffic
CSCvd28859	ASA: PBR Memory leak for ICMP traffic
CSCvd39113	Cluster C-Hash table is updated with one more unit despite the new unit didn't join the setup

Caveat ID Number	Description
CSCvd39113	Cluster C-Hash table is updated with one more unit despite the new unit didn't join the setup
CSCvd43309	Access-lists not being matched for a newly created object-group
CSCvd43309	Access-lists not being matched for a newly created object-group
CSCvd49262	Traceback when trying to save/view access-list with giant object groups (display_hole_og)
CSCvd49262	Traceback when trying to save/view access-list with giant object groups (display_hole_og)
CSCvd50389	RT#687120: Bookmark Issue with clientless VPN - SAML
CSCvd50389	RT#687120: Bookmark Issue with clientless VPN - SAML
CSCvd53884	ASA FirePOWER module data plane down after reload of module
CSCvd53884	ASA FirePOWER module data plane down after reload of module
CSCvd54680	ASA: TLS-proxy - Traceback with thread name - Dispatch Unit
CSCvd54680	ASA: TLS-proxy - Traceback with thread name - Dispatch Unit
CSCvd55115	ASA in cluster results in incorrect user group mappings between the Master and Slave
CSCvd55115	ASA in cluster results in incorrect user group mappings between the Master and Slave
CSCvd55983	Traceback in Thread Name: dhcp_daemon
CSCvd55983	Traceback in Thread Name: dhcp_daemon
CSCvd55999	%ASA-3-216001: internal error in ci_cons_shell: thread data misuse
CSCvd55999	%ASA-3-216001: internal error in ci_cons_shell: thread data misuse
CSCvd58417	DCERPC inspection drops packets and breaks communication
CSCvd58417	DCERPC inspection drops packets and breaks communication
CSCvd62509	ASA traceback in Thread Name: accept/http when ASDM is displaying "Access Rules"
CSCvd62509	ASA traceback in Thread Name: accept/http when ASDM is displaying "Access Rules"
CSCvd65797	ASA May crash when changing a NAT related object to fqdn
CSCvd65797	ASA May crash when changing a NAT related object to fqdn
CSCvd66303	Error deploying ASAv on ESXi vCenter 6.5
CSCvd66303	Error deploying ASAv on ESXi vCenter 6.5
CSCvd76939	ASA policy-map configuration is not replicated to cluster slave

Caveat ID Number	Description
CSCvd76939	ASA policy-map configuration is not replicated to cluster slave
CSCvd78303	ARP functions fail after 213 days of uptime, drop with error 'punt-rate-limit-exceeded'
CSCvd78303	ARP functions fail after 213 days of uptime, drop with error 'punt-rate-limit-exceeded'
CSCvd99476	The interactive icons on internal bookmark site not showing properly (+CSCO+0undefined)
CSCvd99476	The interactive icons on internal bookmark site not showing properly (+CSCO+0undefined)
CSCvd99859	ASA may drop DNS reply containing only additional RR of type TXT
CSCvd99859	ASA may drop DNS reply containing only additional RR of type TXT
CSCve05841	ASA reloaded while joining cluster and active as slave
CSCve05841	ASA reloaded while joining cluster and active as slave

Resolved Bugs in Version 9.4(3)

If you have a Cisco support contract, use the following search for resolved bugs severity 3 and higher for Version 9.4(3):

- [9.4\(3\) fixed bug search](#).

The following table lists resolved bugs at the time of this Release Note publication.

Identifier	Description
CSCsh75522	Increase Content-length counter from 4 to 8 byte size
CSCsl74827	Error messages on console due to QoS configuration
CSCtg74172	Can get around dynamic-filter by using caps in domain name
CSCtj56778	Incorrect ARP MAC Address conversion
CSCtx43501	CPU hog due to snmp polling of ASA memory pool information
CSCtz98516	Observed Traceback in SNMP while querying GET BULK for 'xlate count'
CSCua32157	Remove Code for Type 0 Routing Headers
CSCua32176	IPv6 Complete Packet Fragment Reassembly Check Bypass
CSCub30181	ASA doesn't set ACE inactive when time-range expires
CSCuc11186	ARP: Proxy IP traffic is hijacked.
CSCui20213	5585 interface counters show 0 for working interfaces and console errors
CSCuj04699	ASA WebVPN: Java Signer Certificate chain is incomplete with >3 CA Certs

Identifier	Description
CSCum70304	FIPS self test power on fails - fipsPostDrbgKat
CSCun21186	ASA traceback when retrieving idfw topn user from slave
CSCuo08193	Traceback in Thread Name: DATAPATH-1-1382 while processing nat-t packet
CSCuo85585	ARP debug messages are printing without new line on standby unit
CSCuq21426	Inspect-DNS: PTR Query failed when DNS-Doctoring enabled
CSCuq27723	WebVPN Citrix client browser couldn't save Java Client as preferred
CSCuq27754	WebVPN client browser doesn't show all content from flash site
CSCur07369	SXP Version Mismatch Between ASA & N7K with clustering
CSCur46371	TLSv1.2 Client Cert Auth Connection Establishment Failure
CSCur49234	ASA Mgmt Session stuck on running "sh block exhaustion snapshot/history"
CSCur87011	ASA low DMA memory on low end ASA-X -5512/5515 devices
CSCus08239	ASDM upload causes traceback, OCTEON_CRYPT0: SG buffers exceeds limit
CSCus08552	show traffic protocol stats show large counter values-enhanced pkt stats
CSCus10787	Transactional ACL commit will bypass security policy during compilation
CSCus14568	seamless upgrade on spyker A floods error messages to both asa units
CSCus16416	Share licenses are not activated on failover pair after power cycle
CSCus53126	ASA traffic not sent properly using 'traffic-forward sfr monitor-only'
CSCus65997	Failover State Link Must Support Directly Connected Redundant Interface
CSCut03981	ASA SSLVPN Client cert validation failure - SSL Lib error: Bad RSA Sig
CSCut10103	ASA 5545x Upgrade to 9.2(2)4 causes Traceback in Thread Name SSL
CSCut14209	Cisco ASA XML Denial of Service Vulnerability
CSCut18736	ASA crashes after clear configure all command
CSCut35367	SVG Parser not mangling xlink:href attribute
CSCut40770	Interface TLV to SFR is corrupt when frame is longer than 2048 bytes
CSCut49034	ASA: High CPU on standby due to RDP conn to AC client from CL SSL portal
CSCut67779	Investigate impact of jumbo-frame reservation on low-end ASA platforms
CSCut71095	ASA WebVPN clientless cookie authentication bypass
CSCut74139	Standard Based IKEv2: Incorrect command to configure DPD

Identifier	Description
CSCUu02848	Disable ECDSA SSL Ciphers When Manually Configuring RSA Cert for SSL
CSCUu04012	ASA CX - Data Plane marked as DOWN until ASA reload.
CSCUu48197	ASA: Stuck uauth entry rejects AnyConnect user connections
CSCUu61573	9.5.2 Gold Setup - Traceback in DATAPATH-6-2596 snp_fp_get_frag_chain
CSCUu61981	http servershows as enable in running config while not
CSCUu73395	Auth-prompt configured in one context appears in another context
CSCUu77207	ASA - URL filter - traceback on thread name uauth_urlb clean
CSCUu82229	ikev2 with DH 19 and above fails to pass traffic after phase2 rekey
CSCUu87823	ASAv traceback in DATAPATH when used for WebVPN
CSCUu88412	When > 510 characters entered in CLI, context switches to admin/system
CSCUu91304	Immediate FIN from client after GET breaks scansafe connection
CSCUv05255	ASA built and teardown log messages show "any" information
CSCUv05916	Need to prevent traceback in js_parser_print_rest
CSCUv09538	ASA: CLI commands not showing help(?) options for local authorization
CSCUv09640	ASA: "Auto-Enable" feature not working with SSH configured with PKF
CSCUv11963	TP Auth fails when sub CA using RSA keys is signed by root using ECDSA
CSCUv20449	Traceback in Thread Name: ssh when using capture or continuous ping
CSCUv21478	Cisco ASA tunnel group parameter validation
CSCUv27197	ASA SSLVPN RDP Plugin session freezes under heavy load with activex
CSCUv32615	ASA: LDAP over SSL Authentication failure
CSCUv32789	ASA using IKEv2 rejects more than 10 NAT_DETECTION_SOURCE_IP payloads
CSCUv35050	ASA - slow NFSv3 transfer with sunrpc inspection
CSCUv35243	ASA: Not able to remove ACE with "log default" keyword
CSCUv39775	ASA cluster-Incorrect "current conns" counter in service-policy
CSCUv42720	Egress ACL with ICMP Types Misbehaving.
CSCUv43902	ASA: Watchdog Traceback with Thread Name:- SXP CORE
CSCUv45756	ASA may tracebeck when displaying packet capture with trace option
CSCUv47191	9.5.1 - Crash in bcm_esw_init thread

Identifier	Description
CSCuv49100	ASA: Unable to ping fover IPv6 address in multiple mode
CSCuv49446	ASA traceback on Standby device during config sync in thread DATAPATH
CSCuv50709	Standby ASA inside IP not reachable after Anyconnect disconnect
CSCuv51649	SSL : Unable to Join nodes in Cluster
CSCuv52750	Cannot change "management-only" for port-channel interfaces on 5500-X
CSCuv57389	ASA PKI: cert auth fails after upgrade to 9.1(6.4) / 9.1(6.6) / 9.1(6.8)
CSCuv58559	Traceback in Thread Name: DATAPATH on modifying "set connection" in MPF
CSCuv60724	Cisco ASA Unicast Reverse Path Forwarding (uRPF) Bypass Vulnerability
CSCuv62085	Cisco ASA Clientless SSL VPN portal hangs
CSCuv62204	"show ipv6 neighbor" command not available in system space
CSCuv66333	ASA picks incorrect trustpoint to verify OCSP Response
CSCuv69235	HTTP chunked data causing watchdog
CSCuv70576	Cisco ASA VPN Memory Block Exhaustion Vulnerability
CSCuv70932	FO: ASAv traceback while syncing during upgrade from 9.4.1 to 9.5.1
CSCuv72826	object-group-search access-control enabled, nested object group issue
CSCuv76342	ISA3000 crashed while generating crypto rsa keys
CSCuv79552	Standby traceback during config replication with customization export
CSCuv80580	ASA allows AC session with existing AAA assigned address after failover
CSCuv85752	Group-lock value can be set with space in a tunnel-group name
CSCuv86227	ASA sending incorrect ACL hash for ASDM TopN ACL statistics on a cluster
CSCuv86500	Webvpn: JS parser may crash if the underlying connection is closed
CSCuv87150	ASA traceback in Thread Name: fover_parse (ak47/ramfs)
CSCuv87760	Unicorn proxy thread traceback with RAMFS processing
CSCuv88785	RA validation failed when CA/subCA contains name constraints
CSCuv88898	WEBVPN Rewriter: Stops mangling after hex code of Period on Bookmark URL
CSCuv90156	All Remarks in ACLs are pushed to the end of each ACL after upgrade
CSCuv91730	Request allow packets to pass when snort is down for ASA configurations
CSCuv92371	ASA traceback: SSH Thread: many users logged in and dACLs being modified

Identifier	Description
CSCUv92384	ASA TCP Normalizer sends PUSH ACK for invalid ACK for half-open CONNS
CSCUv93407	ASA Lina: fix memory leak in debug menu option 20
CSCUv94338	ASA traceback in Thread Name: CP Crypto Result Processing.
CSCUv95320	ASA User Ident MAC mismatch remove command not applied
CSCUv96011	OSPF over IKEv2 L2L tunnel is broken on ASA with 9.2.1 onwards
CSCUw00971	ASA truncates url-redirect at 160 chars for ra vpn clients (ISE 1.3+)
CSCUw02009	ASA - SSH sessions stuck in CLOSE_WAIT causing ASA to send RST
CSCUw03367	ASA not installing external LSA with recursive forwarding address
CSCUw03407	DHCPD Search domain shorter than 10 characters is corrupted
CSCUw06294	ASA: Traceback in Thread Name Checkheaps due to webvpn
CSCUw08183	ipAdEntNetMask is not gettable using snmpget with failover IP address
CSCUw09578	ASA 9.3.3.224 traceback in ak47_platform.c with WebVPN stress test
CSCUw14334	Trace back with Thread Name: IP Address Assign
CSCUw15152	Fix broken gcov build in dublin/main
CSCUw15615	Backup unknown with dynamic pat pool
CSCUw16607	ASA EIGRP does not send poison reverse for neighbors to remove route
CSCUw17930	Improper S2S IPSec Datapath Selection for Remote Overlapping Networks
CSCUw19671	ASA traceback while restoring backup configuration from ASDM
CSCUw22130	ASA traceback when removing dynamic PAT statement from cluster
CSCUw24664	ASA:Traceback in Thread Name:- netfs_thread_init
CSCUw26991	ASA: Traceback in Thread Unicorn Admin Handler due to Threat Detection
CSCUw28735	Cisco ASA Software Version Information Disclosure Vulnerability
CSCUw30700	traffic-forward interface command is not working on 5585
CSCUw30999	ASA5508 5516 Unable to communicate with 100/full configured after reboot.
CSCUw32125	ASA stacktrace in vpn client disconnect that had dACL applied
CSCUw32493	ASA BGP peering flaps with password and ikev2 tunnel.
CSCUw33713	IKEv2: crypto iskamp identity auto doesn't work - DN not IKE ID but IP.
CSCUw33860	RA-VPN transactions are shown as 0 in PRSM Dashboard

Identifier	Description
CSCuW36853	ASA: ICMP error loop on cluster CCL with Interface PAT
CSCuW39685	filter sfr traffic may cause memory corruption
CSCuW40468	DHCP proxy overrides chosen DHCP server in multiple DHCP server scenario
CSCuW41548	DNS Traceback in channel_put()
CSCuW44038	Watchdog traceback in ldap_client_thread with large number of ldap grps
CSCuW44744	Traceback in WebVPN rewriter
CSCuW48499	QEMU coredump: qemu_thread_create: Resource temporarily unavailable
CSCuW51333	ASA 9.4 - missing server authenticate-client command for tls proxy
CSCuW51576	SSH connections are not timed out on ASA (stuck in rtcli)
CSCuW55813	Standby ASA traceback in Thread Name: EIGRP-IPv4
CSCuW59382	Rewriter errors when access IEEE website search feature through portal
CSCuW62030	ASA DNS doctoring not working with "any" keyword
CSCuW65183	PBR set ip next-hop lost on boot if name configured for IP argument
CSCuW66397	DHCP Server Process stuck if dhcpd auto_config already enabled from CLI
CSCuW75736	ASA 9.4 - The source of CoA packet does not match tunnel-group config
CSCuW81402	ASA packet-tracer and trace capture incorrect result in case of ECMP
CSCuW82198	Default inspection engines enabled on Standby but not on Active ASA
CSCuW85261	SAML won't be able select Oracle OAM tunnel group
CSCuW87331	ASA: Traceback in Thread name DATAPATH-7-1918
CSCuW87910	PCP 10.6 Clientless VPN Access is Denied when accessing Pages
CSCuW88405	BGP not working when admin context is in transparent mode
CSCuW90116	ASA 9.4.1 traceback upon clearing and reconfiguring ACL
CSCuW92005	Thread Name: DATAPATH-17-3095: ASA in Cluster Reloads Unexpectedly
CSCuW97445	clustering nat : Observing crash on blade after disabling cluster on uut
CSCuX00686	Evaluate CVE-2015-6360 for libsrtp Denial of Service (DoS)
CSCuX03626	Traceback in thread name: Unicorn Proxy Thread
CSCuX05081	RSA 4096 key generation causes failover
CSCuX07002	ASA: assertion "pp->pd == pd" failed: file "main.c", line 192

Identifier	Description
CSCux07478	Session Manager debugs missing identifiers and logoff oldest wrap issue
CSCux08783	CWS: ASA does not append XSS headers
CSCux08838	ASA: Traceback in Checkheaps
CSCux09040	ASA not denying initial SYN to non gateway of host
CSCux09181	http-form authentication fails after 9.3.2
CSCux09310	ASA traceback when using an ECDSA certificate
CSCux11440	ASA traceback in Unicorn Proxy Thread
CSCux12959	"failover standby config-lock" is not loaded in ASA correctly
CSCux16427	PBR incorrect route selection for deny clause
CSCux20178	OSPF neighbor goes down after "reload in xx" commnad in 9.2 and later
CSCux20913	Clustering NAT: ASA crash during NAT configuration
CSCux21955	ASA: FAILOVER not working with password encryption.
CSCux22468	VPN connection may fail when using an ECDSA certificate
CSCux23659	ASA 9.1.6.10 traceback after remove compact flash and execute dir cmd
CSCux26443	DAP URL-List Command Says It Supports 491 Characters; Only Supports 245
CSCux27028	L2TP/IPSec fails with Multilink PPP enabled on Win client
CSCux27903	BOSC Runtime Buffer overflow error detected while executing OSPFV3 Tests
CSCux28324	The copy command does not verify the integrity of the image
CSCux29453	IPv6: ASA denies IPv6-ICMP request to the ASA when failover
CSCux29842	Primary and Secondary ASA in HA is traceback in Thread Name:DataPath
CSCux29929	ASA 9.4.2 traceback in DATAPATH
CSCux29978	Cisco ASA IKEv1 and IKEv2 Buffer Overflow Vulnerability
CSCux33808	ASA ERROR:FIPS Self-Test failure,fips_continuous_rng_test [-1:12:0:2:16]
CSCux33974	ASA "show chunkstat redirect" does not work
CSCux35272	ASA TCP normalizer checksum verification cannot be disabled
CSCux35538	Traceback in ctm_ssl_generate_key with DHE ciphers SSL VPN scaled test
CSCux36112	PBR: Mem leak in cluster mode due to policy based route
CSCux37303	Port-Channel Config on Gi 0/0 causes Boot Loop - FIPS related

Identifier	Description
CSCux37442	Cisco signed certificate expired for WebVpn Port Forward Binary on ASA
CSCux39988	Different output of BVI address in transparent mode on failover pair
CSCux41145	Evaluation of pix-asa for OpenSSL December 2015 Vulnerabilities
CSCux41622	"set connection timeout idle" is not applied.
CSCux41876	ASA IPSEC crypto map set df-bit copy-df/clear-df does not take effect
CSCux42019	Cisco ASA IKEv1 and IKEv2 Buffer Overflow Vulnerability
CSCux42936	ASA 9.5.1 traceback in Threadname Datapath due to SIP Inspection
CSCux43345	Allow a larger (4GB) coredump filesystem to be configured on ASA
CSCux43978	DHCP Relay fails for cluster ASAs with long interface names
CSCux45179	SSL sessions stop processing -"Unable to create session directory" error
CSCux46192	ASA coredumped after enable/disable webvpn on interface
CSCux47195	ASA(9.5.2) changing the ACK number sent to client with SFR redirection
CSCux50234	asa fails to format disk1 USB drive
CSCux55923	WebVPN: Unable to play certain online videos
CSCux56111	"no ipv6-vpn-addr-assign" CLI not working
CSCux58172	DAP: debug dap trace not fully shown after +1600 lines
CSCux59122	ASA L7 policy-map comes into affect only if the inspection is re-applied
CSCux61257	ASA: Traceback in Thread IP Address Assign
CSCux63532	webvpn cache-disabled msg is too disruptive and may cause config issues
CSCux63770	IPAA needs improved debugging - Part 2- add Syslogs 737034-737036
CSCux64134	Incorrect NTP authentication behavior
CSCux66866	Traffic drop due to constant amount of arp on ASASM
CSCux69987	ASA: Traceback on ASA device after adding FQDN objects in NAT rule
CSCux70784	ASA Crash while viewing large ACL
CSCux70993	ASA unable to add policy NAT which is overlapping with ip local pool
CSCux70998	Reload in Thread Name: IKE Daemon
CSCux71197	"show resource usage" gives wrong number of routes after shut/no sh
CSCux72610	ASA TACACS+: process tacplus_snd uses large percentage of CPU

Identifier	Description
CSCux81075	PBR "set interface" failing to use default and less preferred route
CSCux81683	ASA Traceback on Thread Name: Unicorn Admin Handler
CSCux82023	Stub Connections Torn Down due to Shun/Threat Detection in ASA Cluster
CSCux82835	Nat pool exhausted observed when enabling asp transactional-commit nat
CSCux83705	DNS Reply Modification for Dual-Stack does not work as expected
CSCux85725	ASA WebVPN: Java RDP Plugin does not launch
CSCux85863	FIPS: Continuous RNG test can mistakenly report an error
CSCux87457	ASA traceback in Thread Name: https_proxy
CSCux88237	ASA traceback in DATAPATH thread
CSCux90740	"backup" command does not include anyconnect client profile files
CSCux90767	Resolve CSCtz82865 - Equivalent of "show xlate count" command
CSCux93751	Cisco ASA Linux Kernel Vulnerability - CVE-2016-0728
CSCux94598	ASA using a huge dynamic ACL may cause Anyconnect connectivity failures
CSCux99214	ASA5516 SSD reports incorrect OID in Entity MIB
CSCux99392	Uploaded/downloaded files via CIFS have Zero Byte size (same WebFolder)
CSCuy01420	ASA traceback in Thread Name: Unicorn Proxy Thread.
CSCuy03024	ASA traceback and reload citing Thread Name: idfw_proc
CSCuy05949	ASA: MAC address changes on active context when WRITE STANDBY is issued
CSCuy07753	Smart tunnel does not work since Firefox 32bit version 43
CSCuy08051	9.5(1) ECDSA CSR sets KU KeyEnciph vice KeyAgreement
CSCuy10929	Not able to re-use the community-list name.
CSCuy11281	ASA: Assert traceback in version 9.4.2
CSCuy11905	ASA 5585 traceback when the User name is mentioned in the Access list
CSCuy13937	ASA Watchdog traceback in CP Processing thread during TLS processing
CSCuy21287	STBY ASA doesn't pass traffic via ASA-IC-6GE-SFP-B ifc after reload
CSCuy22561	VPN Load-Balancing does not send load-balancing cert for IPv6 Address
CSCuy30069	ASA 9.5.2 does not send CERT_REQ for 512-bit certificate
CSCuy32321	Traceback in ldap_client_thread with ldap attr mapping and pw-mgmt

Identifier	Description
CSCuy34265	ASA Access-list missing and losing elements after configuration change
CSCuy36897	Can't navigate to OWA 2013 due to ssl errors
CSCuy41986	OCSP validation fails when multiple certs in chain are verified
CSCuy43839	ASA reloads in thread name: DATAPATH while encrypting L2L packet
CSCuy43857	ASA WebVPN: Java Exception with Kronos application
CSCuy49902	inspect ip-option is not allowing "NOP" even when allowed
CSCuy51918	Buffer overflow in RAMFS dirent structure causing traceback
CSCuy62198	If FQDN is more than 64 chars then we redirect to ip instead of FQDN
CSCuy65416	assert "ctm->async_ref == 0" failed: file "ssl_common.c", line 193-part2
CSCuy73652	Traceback in thread name idfw when modifying object-group having FQDN
CSCuy74218	Assert Traceback in Thread Name: DATAPATH on clustered packet reassembly
CSCuy74362	WebVPN FTP client failing with "Error contacting host" message
CSCuy78802	original master not defending all GARP packets after cluster split brain
CSCuy80058	FO replication failed: cmd=no disable, when disabling webvpn-cache
CSCuy84044	Rewriter error with webworker JS
CSCuy85243	ASA traceback when receive Radius attribute with improper variable type
CSCuy88971	ASA does not suppress EIGRP candidate default route information
CSCuy96391	ASA clientless rewriter failure at 'CSCOPut_hash' function
CSCuy99280	ENH: ASAv should have a different pre-loaded cert
CSCuz10371	ASA Traceback and reload by strncpy_sx.c
CSCuz18707	Intranet page does not load via WebVPN with JavaScript errors
CSCuz21068	CSCOPut_hash can initiate unexpected requests

Resolved Bugs in Version 9.4(2.145)

There were no bugs fixed in 9.4(2.145).

Resolved Bugs in Version 9.4(2)

If you have a Cisco support contract, use the following search for resolved bugs severity 3 and higher for Version 9.4(2):

- [9.4\(2\) fixed bug search](#).

The following table lists resolved bugs at the time of this Release Note publication.

Identifier	Description
CSCtg74172	Can get around dynamic-filter by using caps in domain name
CSCti05769	Migration of max_conn/em_limit to MPF is completely wrong in 8.3
CSCtq90780	ASA allows removing address pool conf even if it is in use in grp-policy
CSCtr84992	Possible to add multiple identical lines under certificate maps
CSCty02525	Last transaction time in 'show aaa-server' cmd changes.
CSCtz98516	Observed Traceback in SNMP while querying GET BULK for 'xlate count'
CSCua32157	Remove Code for Type 0 Routing Headers
CSCua32176	IPv6 Complete Packet Fragment Reassembly Check Bypass
CSCuc02113	ISAKMP debugs display incorrect Message ID and length data
CSCuc16228	Can't use an object-group for NAT which was used for pat-pool earlier
CSCuc16662	HTML/Java File Browser- created file or folder shows 9 months offset
CSCui37201	Misleading error msg for pat-pool with mapped object
CSCui71332	IPv6 ND not replicating to Slave units
CSCuj04699	ASA WebVPN: Java Signer Certificate chain is incomplete with >3 CA Certs
CSCuj68919	Multiple problems with output of show processes memory
CSCul02601	Cisco ASA SNMP Denial of Service Vulnerability
CSCup89922	ASA DNS lookups always prefer IPv6 response
CSCuq09430	ASA "debug webvpn anyconnect 255" not showing empty certificate issue
CSCuq10239	Windows 8 with new JRE, IE is not gaining access to smart tunnel
CSCuq27342	Traceback and reload triggered by failover configuration
CSCuq27723	WebVPN Citrix client browser couldn't save Java Client as preferred
CSCuq57307	ASA 8.4 Memory leak due to duplicate entries in ASP table
CSCuq97035	WEBVPN: Citrix 5/6 application doesn't launch with IE10/Windows 7
CSCuq99821	ASA/ASASM drops SIP invite packets with From field containing "" and \
CSCur07061	Traceback on standby ASA during hitless upgrade
CSCur07369	SXP Version Mismatch Between ASA & N7K with clustering
CSCur09141	RRI static routing changes not updated in routing table

Identifier	Description
CSCur17006	Add cli to control masked username in syslog
CSCur20322	ASA 9.2.1 - DATAPATH Traceback in L2 cluster environment
CSCur21069	Cisco ASA Failover Command Injection Vulnerability
CSCur51051	LU allocate connection failed on the Standby ASA unit
CSCur56038	RPC error in request config after replicated a large configuration
CSCur68866	QEMU virtqueue_map_sg() Function Input Validation Buffer Overflow Vuln
CSCur99221	NetFlow incorrect reporting for PPTP VPN over GRE
CSCur99653	Codonomicon HTTP-server suite may cause crash
CSCus06165	ASA:Dataplane capture doesn't capture packets From Service module to ASA
CSCus08239	ASDM upload causes traceback, OCTEON_CRYPT0: SG buffers exceeds limit
CSCus14568	seamless upgrade on spyker A floods error messages to both asa units
CSCus19673	"no nameif" is removing the policy-route configuration
CSCus22893	Extra space after newline in some syslogs
CSCus23248	Cisco ASA DHCPv6 Relay DoS Vulnerability
CSCus27650	Cut Through proxy not working correctly with TLS1.2
CSCus32005	ASA - Traceback in thread name SSH while applying BGP show commands
CSCus37840	AnyConnect upgrade from AC 2.5 to AC 3.1 fails
CSCus46895	WebVPN Rewriter: "parse" method returns curly brace instead of semicolon
CSCus47259	Cisco ASA XAUTH Bypass Vulnerability
CSCus49405	SCH enrollment issue with Saleen serial number
CSCus53692	ASA traceback in Thread Name: fover_parse
CSCus56252	Cisco ASA DHCPv6 Relay Denial of Service Vulnerability
CSCus56590	ASA - Traceback in Thread Name: fover_parse
CSCus62863	Kenton 5516: Interface dropping ARPs after flapping under traffic load
CSCus62884	ASA 9.1.5 does not always drop connections after receiving RST+ACK flag
CSCus63269	HTTP redirect to the VPNLB address using HTTPS fails in 9.1.5
CSCus63993	ASA - Traceback in thread name: CERT API
CSCus64394	Misleading route-map warning message

Identifier	Description
CSCus69021	5506-X: 'no buffer' interface counter reports incorrect errors
CSCus70693	ASA 9.3.2 SSL doesn't work with error: %ASA-4-402123: CRYPTO:
CSCus71190	LDAP over SSL fails when using TLS1.2 on ASA
CSCus73422	Close-overlay function not working thru rewriter
CSCus74398	Cisco ASA PIM Multicast Registration Vulnerability
CSCus76060	ASA clears the TOS value of ICMP echo reply packet from ASA's interface
CSCus76632	assertion "mh->mh_mem_pool>MEMPOOL_UNDEFINED&&mh->mh_mem_pool<MEMP
CSCus78450	ASA cert validation fails when suitable TP is above the resident CA cert
CSCus78722	inspect esmtp replace the packet data to 'X'
CSCus79129	ASAv crashes when CiscoTAC-1 profile pointed to Transport Gateway w/ dbg
CSCus83476	More than 255 messages in multicast packet with jumbo frames
CSCus83942	ASA : ACL logging is not getting disabled with keyword "log disable"
CSCus84220	ASA crashes for the OSPFv2 packets from codenomicon
CSCus85532	IKEv2: IPsec SA's are created by dynamic crypto map for static peers
CSCus86487	PBR: DF & DSCP bits are not getting set without valid set next-hop
CSCus88626	Radius Acct-Terminate-Cause for L2TP over IPsec is incorrect.
CSCus88641	Memory leak observed while adding manual NAT rule
CSCus89139	Exception on asdm_handler stream line: </threat-detection>
CSCus89286	ASA Traceback in SSL library due to DMA memory exhaustion
CSCus91407	Network Object NAT is not working when config-register == 0x41
CSCus91636	Adding subnet(s) to the object group for NAT causes high CPU
CSCus92570	'client-services' is not accepted if the interface has no IP addr
CSCus92856	ASA traceback in DATAPATH Thread due to Double Block Free
CSCus94026	Cisco ASA ISAKMP Denial of Service Vulnerability
CSCus95290	Cisco ASA VPN XML Parser Denial of Service Vulnerability
CSCus97061	ASA Cluster member traceback in DATAPATH
CSCus98250	ASA WEBVPN: Usernames shown as '*' in logs for failed authentication

Identifier	Description
CSCus98309	Duplicate IPv6 address is configurable in 1 ASA or context
CSCut01395	ASA silently dropping OSPF LS Update messages from neighbors
CSCut01856	ASA dropping traffic with TCP syslog configured in multicontext mode
CSCut03495	Cisco ASA DNS Denial of Service Vulnerability
CSCut03981	ASA SSLVPN Client cert validation failure - SSL Lib error: Bad RSA Sig
CSCut04182	NFS connections not timing out after failover
CSCut04996	DHCPRelay Server in interface mode not getting deleted
CSCut05676	Handling esmtp default parameters for TLS
CSCut06531	ASA: XFRAME support for .JS and .JNLP URL's
CSCut08663	Both ASAs in failover use the same MAC address
CSCut10078	Standby ASA does not apply OSPF route after config replication
CSCut11895	Failover assembly remained in active-active state permanently
CSCut12513	ASA allows citrix ICA connection without authentication
CSCut14223	Cisco ASA Management Interface XML Parser DoS Vulnerability
CSCut15570	Anyconnect SSL VPN certificate authentication fails o ASA
CSCut22865	[ASA] CTP not working if proxyACL port_argument is gt
CSCut23991	PPPoE session state timer does not initialize properly
CSCut24490	L2TP/IPSec Optimal MSS is not what it's supposed to be
CSCut26062	xsZASA 9.2.1 Eigrp Authentication does not work with 16 character key
CSCut27332	ASA traceback in aaa_shim_thread / command author done for dACL install
CSCut28210	AAA: RSA/SDI integration failing with ASA 9.3(2) - node secret issue
CSCut28217	Active ASA in failover setup reboots on its own
CSCut30741	ASA redirection to Scansafe tower fails with log id "775002" in syslog
CSCut31315	[ASA] access-list ACL_name standard permit host 0.0.0.0 deleted
CSCut35406	Src url of video track tag not mangled via webvpn
CSCut36927	Cluster destabilizes when contexts are removed
CSCut37042	Secondary ASA stuck in config sync while upgrading to 8.4.x
CSCut37974	EIGRP authentication not working with simple password

Identifier	Description
CSCut39169	WebVPN:Rewrite issue with 'eval' expressions inside JS on Peoplesoft app
CSCut39985	Per-session PAT RST sent to incorrect direction after closing session
CSCut44075	Traceback in snp_cluster_get_buffer
CSCut44082	EIGRP configuration not being correctly replicated between failover ASAs
CSCut45114	2048-byte block leak if DNS server replies with "No such name"
CSCut46019	MARCH 2015 OpenSSL Vulnerabilities
CSCut48009	Traceback in thread CP Processing
CSCut48571	Incorrect cert chain sent to connecting IPsec clients
CSCut49034	ASA: High CPU on standby due to RDP conn to AC client from CL SSL portal
CSCut49111	ASA traceback because of TD tcp-intercept feature
CSCut49711	show cluster mem indicates incorrect values
CSCut49724	Corrupted host name may occur with DHCP
CSCut52679	Cisco ASA OSPFv2 Denial of Service Vulnerability
CSCut54218	ASA tunnel-group"password-expire-in-days"not prompting a password change
CSCut56198	Clustering: Traceback in DATAPATH with transparent FW
CSCut58935	WebVPN: Tswb fails to work through clientless portal
CSCut64327	L2TP/IPsec traffic dropped due to "vpn-overlap-conflict"
CSCut64846	To-the-box UDP traffic not getting inspected and getting dropped on ASA
CSCut67315	ASA :Top 10 Users status is not getting enabled from ASDM.
CSCut67779	Investigate impact of jumbo-frame reservation on low-end ASA platforms
CSCut67965	CRYPTO_PKI: ERROR: Unable to allocate new session. Max sessions reached
CSCut69675	Radius Acct-Terminate-Cause for L2TP over IPsec is incorrect.
CSCut71095	ASA WebVPN clientless cookie authentication bypass
CSCut75202	PKI: potential pki session handle leak in IKEv2 L2L configurations
CSCut75983	ASA Traceback in PPP
CSCut80316	Ikev2 Session with bogus assigned IP address stays on ASA
CSCut83833	USB device hot plug not supported in running ASA
CSCut85049	Issue with downloading images from Sharepoint

Identifier	Description
CSCut86523	ASA: Silently Drops packets with SFR Module installed.
CSCut88287	ASA Traceback in vpnfol_thread_msg
CSCut92194	ASA traceback in Thread Name: CP Processing
CSCut92373	ASA 9.0.3 not logging permitted UDP traffic
CSCut95793	ASA: Anyconnect IPv6 Traceroute does not work as expected
CSCut96928	ASA : Password creation date is decrementing by one with every reboot
CSCuu00733	ASA: ECMP stopped working after upgrade to 9.3.2
CSCuu02635	Remove demo and eval warning for sfr monitor-only
CSCuu02761	DNS should perform IPv4 lookups if IPv6 address is not reachable
CSCuu04160	snmpwalk causes slow memory leak on ASA
CSCuu07308	"ssh scopy enable" deleted from configuration
CSCuu07462	Cannot bootup ASAv-KVM when deployed via RHEL (7.1) / OpenStack (Juno)
CSCuu07799	Cisco ASA DNS Denial of Service Vulnerability
CSCuu08031	ASA QoS Priority Queue tx-ring-limit 512 causes high impact to LLQ
CSCuu09302	ASAv: RSA key pair needs to be automatically generated with 2048 bits
CSCuu10284	ASA Dataplane captures dont capture packets when using match/access-list
CSCuu13345	Drop reasons missing from asp-drop capture
CSCuu16983	ASA: failover logging messages appear in user context
CSCuu18527	ASA WebVPN: HTTP 302 Location URL rewritten incorrectly
CSCuu18564	ASA WebVPN : jQuery based Calendar table fails to load; Empty frame
CSCuu18989	ASA %ASA-3-201011: Connection limit exceeded when not hitting max limit
CSCuu19489	ASA inspection-MPF ACL changes not inserted into ASP table properly
CSCuu25430	Object nat rule is not matched
CSCuu27334	ASA: Traceback with Thread Name - AAA
CSCuu28909	ASA cluster: ICMP loop on CCL for ICMP packet destined to the VPN tunnel
CSCuu31281	AAA Authorization HTTP sends username in password field of authorization
CSCuu31751	ASA OSPF database not reflect changes
CSCuu32905	ASA WebVPN: Javascript fails to execute when accessing internal portal

Identifier	Description
CSCuu36639	ASA 5506X: ESP Packet drop due to crypto accelerator ring timeout
CSCuu39615	eglibc 2.18 is missing upstream fix #15073
CSCuu39636	Cert Auth fails with 'max simultaneous-login restriction' error
CSCuu41142	IPv6 local host route fail when setting link-local/Global simultaneously
CSCuu45812	asa Traceback with Thread Name idfw_proc
CSCuu45813	ASA Name Constraints dirName improperly verified
CSCuu45858	ASA Traceback in cp_syslog
CSCuu46569	ASA CA certificate import fails with different types of Name Constraints
CSCuu48626	ASA - access list address argument changed from host 0.0.0.0 to host ::
CSCuu48813	WebVpn: portal is not displayed after re-login
CSCuu52976	ASA not checking the MAC of the TLS records
CSCuu53928	ASA does not set forward address or p-bit in OSPF redistribution in NSSA
CSCuu54046	All Static routes not removed on adding zone membership to an interface
CSCuu54660	ASA Remote Access - Phase 1 terminated after xauth
CSCuu56912	ASA change non-default port to 443 for https traffic redirected to CWS
CSCuu61573	9.5.2 Gold Setup - Traceback in DATAPATH-6-2596 snp_fp_get_frag_chain
CSCuu63656	ASA not generating PIM register packet for directly connected sources
CSCuu66218	ASA is not correctly handling errors on AES-GCM ICV
CSCuu73087	Standalone AnyConnect fails to connect due to empty DAP user message
CSCuu73395	Auth-prompt configured in one context appears in another context
CSCuu73716	Traceback in Thread CP Processing
CSCuu74823	Cryptomaps lose trustpoint when syncing configuration from cluster unit
CSCuu75675	kenton: For ASA5516, ASAOS should support SSLVPN of 300 instead of 250
CSCuu75901	ASA failover due to issue show local-host command make CPU-hog
CSCuu76651	Traps are not sent after hyperlite bootup with all data interfaces shut
CSCuu77207	ASA - URL filter - traceback on thread name uauth_urlb clean
CSCuu78835	Webvpn rewrite issues for Confluence - by atlassian on latest v6.4.5
CSCuu81932	ASA tunnel-group-map cannot contain spaces

Identifier	Description
CSCuu83280	Evaluation of OpenSSL June 2015
CSCuu84085	DHCP-DHCP Proxy thread traceback shortly after failover and reload
CSCuu84697	ASA Traceback in Thread Name ssh/client
CSCuu86195	conn-max counter is not decreased accordingly
CSCuu87823	ASAv traceback in DATAPATH when used for WebVPN
CSCuu88548	Ampersand (&) not encoded in packet tracer phase 'extra' field
CSCuu88607	Doubling counting flow bytes for decrypted packets
CSCuu92632	ASA sets non-zero FA in OSPF for anyconnect redistributed network
CSCuu93339	Cisco ASA Poodle TLS Variant
CSCuu94945	ASA: Traceback while copying file using SCP on ASA
CSCuu96492	'terminal pager' does not clear when authorization auto-enable is used
CSCuu97304	SSL connection failing to WebVPN portal
CSCuu99349	ASA-3-317012 and "No route to host" errors even though the route exists
CSCuu99902	Saleen Alarm LED lit when BMC SEL log is full
CSCuv01022	ASA:OSPF over L2L tunnels is not working with multiple cry map entries
CSCuv01177	ASA: traceback in IDFW AD agent
CSCuv02304	EEM action not executed on absolute time when NTP is configured
CSCuv02619	Standby ipv6 address setting is not replicated to standby
CSCuv05386	Clientless webvpn on ASA does not display asmx files
CSCuv05916	Need to prevent traceback in js_parser_print_rest
CSCuv07106	ASATraceback in ssh whilst adding new line to extended ACL
CSCuv07126	ikev2 enable added to config when zones are used despite ERROR msg
CSCuv09538	ASA: CLI commands not showing help(?) options for local authorization
CSCuv09640	ASA: "Auto-Enable" feature not working with SSH configured with PKF
CSCuv10258	ASA5505 permanent base license, temp secplus, failover, vlan count issue
CSCuv10938	'redistribute' cmds under 'router eigrp' removed on deleting any context
CSCuv11566	ASA LDAP CRL query baseObject DN string is malformed
CSCuv11963	TP Auth fails when sub CA using RSA keys is signed by root using ECDSA

Identifier	Description
CSCuv12564	Memory leak @regcomp_unicorn with APCF configured
CSCuv12884	Unable to authenticate with remove aaa-server from different context
CSCuv13998	ASA : Unable to save configuration or copy files on ASA flash
CSCuv23931	ASA: TLS-Proxy fails with pkp error
CSCuv25327	bgp ipv6 neighborhood fails with ASA after hard reset on router
CSCuv27197	ASA SSLVPN RDP Plugin session freezes under heavy load with activex
CSCuv30184	AddThis widget is not shown causing Traceback in Unicorn Proxy Thread
CSCuv32615	ASA: LDAP over SSL Authentication failure
CSCuv32789	ASA using IKEv2 rejects more than 10 NAT_DETECTION_SOURCE_IP payloads
CSCuv34906	IPv6 packets with a next header of 8 is dropped by failover code
CSCuv35243	ASA: Not able to remove ACE with "log default" keyword
CSCuv38654	rewriter returns 302 for a file download
CSCuv39775	ASA cluster-Incorrect "current conns" counter in service-policy
CSCuv42413	Dynamic Route Not Installed After Failover
CSCuv43902	ASA: Watchdog Traceback with Thread Name:- SXP CORE
CSCuv45756	ASA may traceback when displaying packet capture with trace option
CSCuv51649	SSL : Unable to Join nodes in Cluster
CSCuv52750	Cannot change "management-only" for port-channel interfaces on 5500-X
CSCuv57389	ASA PKI: cert auth fails after upgrade to 9.1(6.4) / 9.1(6.6) / 9.1(6.8)
CSCuv60724	Cisco ASA Unicast Reverse Path Forwarding (uRPF) Bypass Vulnerability
CSCuv62085	Cisco ASA Clientless SSL VPN portal hangs
CSCuv62204	"show ipv6 neighbor" command not available in system space
CSCuv69235	HTTP chunked data causing watchdog
CSCuv70576	Cisco ASA VPN Memory Block Exhaustion Vulnerability
CSCuv79552	Standby traceback during config replication with customization export
CSCuv85752	Group-lock value can be set with space in a tunnel-group name
CSCuv86500	Webvpn: JS parser may crash if the underlying connection is closed
CSCuv87760	Unicorn proxy thread traceback with RAMFS processing

Identifier	Description
CSCuv88785	RA validation failed when CA/subCA contains name constraints
CSCuv90156	All Remarks in ACLs are pushed to the end of each ACL after upgrade
CSCuv91730	Request allow packets to pass when snort is down for ASA configurations
CSCuv93407	ASA Lina: fix memory leak in debug menu option 20
CSCuw00971	ASA truncates url-redirect at 160 chars for ra vpn clients (ISE 1.3+)
CSCuw06294	ASA: Traceback in Thread Name Checkheaps due to webvpn
CSCuw09578	ASA 9.3.3.224 traceback in ak47_platform.c with WebVPN stress test
CSCze96017	Active ftp-data is blocked by Firepower on Chivas Beta on 5512

Resolved Bugs in Version 9.4(1.225)

There were no bugs fixed in 9.4(1.225).

Resolved Bugs in Version 9.4(1.200)

There were no bugs fixed in 9.4(1.200).

Resolved Bugs in Version 9.4(1.152)

There were no bugs fixed in 9.4(1.152).

Resolved Bugs in Version 9.4(1)

If you have a Cisco support contract, use the following search for resolved bugs severity 3 and higher for Version 9.4(1):

- [9.4\(1\) fixed bug search](#).

The following table lists resolved bugs at the time of this Release Note publication.

Identifier	Description
CSCsu40454	UDP telnet/ftp/http/https intercepted for auth-proxy
CSCsy50489	.pkcs12 should not be retrieved after ca enrollment-retrieval timeout
CSCtr95845	TACACS+ Failure to verify reply type
CSCtt88306	Syslog 106100 not generated on second context when cascading contexts.
CSCtu30620	Missing input validation for specific code functions
CSCtw97592	%ASA-6-603106 and %ASA-6-603108 message is printed on 3 lines
CSCub53088	Arsenal:twice NAT with service type ftp not working.
CSCuc80004	Traceback seen when editing ACL configured in AAA UAuth

Identifier	Description
CSCud78760	ASA: Change warning message when L2L tunnel-group is named
CSCue76550	ASA displays incorrect auth type in some IKEv2 L2L configurations
CSCuf03528	Cluster NTP configuration not replicated to slave after unit reloads
CSCuf21519	WebVPN: Latest JQuery library doesn't work through ASA
CSCuf31607	Linux Kernel Invalid fs and gs Registry KVM Denial of Service Vulnerab
CSCuf31726	uLinux Kernel agp_generic_remove_memory() Local Privilege Escalation Vu
CSCug51375	ASA SSL: Continues to accept SSLv3 during TLSv1 only mode
CSCui27525	Idle timer and half-closed idle timer reset by out of sequence SYN
CSCui41969	Authentication is successful, but http browser with error msg displayed
CSCui71332	IPv6 ND not replicating to Slave units
CSCul02601	Cisco ASA SNMP Denial of Service Vulnerability
CSCum63039	Assert in CTM Daemon
CSCun43072	ASA5585-SSP60 Traceback in Thread Name SSH on Capture Command
CSCun45787	Duplicated CHILD SAs in 1 IKEv2 SA, traffic dropped vpn-overlap-conflict
CSCun64754	ASA may traceback when "write standby" command is entered twice
CSCun88736	ASA does not recognise "packet too big" for assembled ICMPv6 echo reply
CSCuo45321	ASA allows IKEv1 clients to bypass address assignment, causing conflict
CSCuo58584	Cisco ASA fix for CSCun56954
CSCuo65775	Cisco ASA Information Disclosure Vulnerability
CSCup15680	TLS-proxy capture decodes not handling large SIP segments
CSCup47195	ASA - Traceback in DATAPATH-0-1275
CSCup73524	HA: "Interfaces on Active and Standby are not consistent" Message on MFM
CSCup87430	accounting not per rfc in dual factor auth case
CSCup92782	ASA providing inaccurate Tunnel count to ASDM
CSCup95504	ASA drops DNS PTR Reply w/ reason Label length exceeded during rewrite
CSCuq12166	"verify /signature running" command output does not show via ssh
CSCuq20396	Traceback when executing "show crypto accelerator load-balance"
CSCuq21016	Local pool address not released -> Duplicate local pool address found

Identifier	Description
CSCuq22357	SCP copy operations exposes sensitive information in syslogs
CSCuq27342	Traceback and reload triggered by failover configuration
CSCuq32943	ASA as DHCP relay, DHCP offer is not forwarded to the client
CSCuq33451	ASA: Increased processor temperature after upgrade
CSCuq35126	PPPoE with static IP address deny packets after reload ASA
CSCuq36615	Traceback caused by WCCP
CSCuq37448	Cisco ASA Failover IPSEC does not encrypt failover link
CSCuq37873	ASA : timeout floating-conn not working when PPPoE is configured
CSCuq39567	Traceback in Thread Name qos_metric_daemon caused by asdm history enable
CSCuq44875	ASA: CLI commands are not displaying options for local authorization
CSCuq45848	TLS proxy packet capture incorrectly displays IPv6 packets in wireshark
CSCuq47381	DMA memory leak in 256 byte fragments with nbns-server config
CSCuq49455	ASA not sending RST packet for connections dropped by Botnet filter
CSCuq50366	Traceback may occur on bring up of multiple SSL sessions w/DHE
CSCuq53421	ASA can use wrong trustpoint with rekeyed CAs are cfg in trustpoints.
CSCuq53636	ASA not sending PIM register message to RP
CSCuq59114	ASA traceback in cluster with DATAPATH thread
CSCuq59667	ASA tracebacks in Thread Name: ssh due to watchdog
CSCuq62164	IPv6 stateless autoconfiguration fails if managed config flag in RA
CSCuq62597	ASA L2TP Split-Tunnel DHCP: DHCP daemon got msg for uninitialized
CSCuq62925	ASA: standby traceback during replication of specific privilege command
CSCuq65201	ASA Local CA generates unexpected renewal reminder message
CSCuq65542	Cisco ASA Software Version Information Disclosure Vulnerability
CSCuq66078	Traceback in clacp_enforce_load_balance with ASA Clustering
CSCuq68271	ASA Cluster slave unit loses default route due to sla monitor
CSCuq68888	Cisco ASA SSL VPN Memory Blocks Exhaustion Vulnerability
CSCuq69907	ASA traceback: thread name "scansafe_poll"
CSCuq72664	ASA - 80 Byte memory block depletion

Identifier	Description
CSCuq75981	ASA traceback in DATAPATH-0-2078 thread
CSCuq76847	ASA:Page fault traceback ACL FQDN Object-group
CSCuq77011	Clientless WebVPN Session Cookie should have configurable HttpOnly flag
CSCuq77228	ASA Cluster: IDFW traceback inThread Name: DATAPATH-3-132
CSCuq77655	Cisco ASA DNS Memory Exhaustion Vulnerability
CSCuq78238	Inspect rule defaults in standby transparent context on write standby
CSCuq80639	ASA5580 speed nonegotiate settings kept link down after shut/no shut
CSCuq87632	User membership not updated in parent group
CSCuq91793	ASA: RST packet forwarded with non-zero ACK number (and ACK flag clear)
CSCuq95704	There are two certificates related to one trustpoint on standby unit.
CSCuq98633	Object Group Search causing legitimate traffic to be dropped by ACL
CSCuq99852	Traceback on ASA when Attempting to Join Cluster with Low Memory
CSCur02239	ASA ACL hitcount not correct for ACLs with service object groups
CSCur07061	Traceback on standby ASA during hitless upgrade
CSCur10595	ASA cut-through proxy limiting authentication attempts from user
CSCur13455	WebVPN Citrix IPv6 connections fail
CSCur16308	DHCP Relay reloads after changing server interface
CSCur17329	SDI authentication doesn't work in more than one contexts.
CSCur17483	nested custom write functions causing blank page through rewriter
CSCur20461	ASA Threat detection adds Shun entry for attacker based on routing table
CSCur21069	Cisco ASA Failover Command Injection Vulnerability
CSCur23709	ASA : evaluation of SSLv3 POODLE vulnerability
CSCur24059	Control Plane ACL Not Working for Redirected HTTP Traffic
CSCur25431	ASA assert traceback on Standby Unit in c_idfw.c
CSCur25542	Traceback: pki-crl: Thread Name: Crypto CA with traffic through VPN L2L
CSCur27553	SCH not using trustpool after trustpoint expiration failure
CSCur27845	ASA Client login timeout issue due to proxy match inconsistency
CSCur28194	Evaluate OpenSSL DTLS SRTP Memory Leak - CVE-2014-3513

Identifier	Description
CSCur28615	Hex code associated with syslog is referenced from the old ACE/ACL
CSCur29644	Evaluate Session Ticket Memory Leak (CVE-2014-3567)
CSCur36898	EIGRP tag incorrectly send by ASA
CSCur38451	ASA DSCP marking applies to all SSL traffic
CSCur38637	CoA: ASA terminates AC SSL session w/out ACL after second CoA update
CSCur40249	L2L Test w/ DFP, SFR and debug SFR results in ASA becoming unresponsive
CSCur41860	HTTP and FTP Copy operations exposes sensitive information in syslogs
CSCur42776	Mac version smart-tunnel uses SSLv3 which is a vulnerability
CSCur42907	Failed to allocate global ID when adding service-policy
CSCur42998	traceback @ hash_table_simple.c:192
CSCur45455	ASA crashes in DHCPV6 Relay agent feature Functionality
CSCur47804	ASA Crash in vpnfol_thread_msg thread
CSCur49086	Traceback due to fiber_create failure in unicorn remove session dir
CSCur52712	Webvpn: Support for XFRAME for non-critical URL's
CSCur52719	webvpn href with javascript function - arg ' incorrectly rewritten to \'
CSCur54570	ASA accounting request does not contain radius-class(25) attribute
CSCur55388	Usernames obscured with asterisks in logs after upgrade to ASA 9.1(5.16)
CSCur56038	RPC error in request config after replicated a large configuration
CSCur56689	inspect conn not replicated to standby with cut_thru missing punt
CSCur57143	ASA/SFR data plane connection may drop under heavy load
CSCur59397	ASA SCP Client does not prompt for password when not inc. in copy string
CSCur59704	ASA: Traceback in idfw_proc
CSCur63365	WebVPN: Cannot use non-default FTP port for filebrowsing
CSCur64589	DATAPATH Traceback in snp_mp_svc_udp_upstream_data function
CSCur64659	ASA Traceback in Thread Name: DATAPATH-6-2544
CSCur65317	NAT pool address distribution fails,with NATtransactional-commit enabled
CSCur66635	ASA Traceback in Thread Name: DATAPATH-3-1274
CSCur68226	ASA SMTP inspection should not disable TLS by default

Identifier	Description
CSCur69227	ASA sporadic crypto errors with SSL VPN using TLS1.x DHE ciphers
CSCur69803	acl rules are not removed when service object-group entry is deleted.
CSCur71254	ASA crash loop while upgrading when FIPS enabled
CSCur75774	ACL Hash not updated when object is renamed
CSCur76771	scansafe feature is missing from registered module features
CSCur77736	ASA : 256 Byte Block Depletion with CoA enabled
CSCur81376	ASA traceback in Thread Name: ci/console, assertion "snp_sp_action.c"
CSCur85582	OSPF over L2L tunnels is broken on ASA in 9.2.1 onwards
CSCur86788	ASA5506: Packet-tracer shows output interface as "NP Identity Ifc"
CSCur87061	Potential ICMP error storm in cluster CCL link
CSCur88829	ASA IPSEC client PKI username from certificate authorization failure
CSCur93251	ASA: Traceback while changing the Ikev1 configuration
CSCur94037	NTP authentication config replication fails in ASA failover and cluster.
CSCur94645	ASA - Additional empty fields in RADIUS Access-Request packet
CSCur95551	ASA prefers Suite-B algorithms w/ AC Essentials enabled for AC IKEv2
CSCur98502	ASA: 'no monitor-interface service-module' command gone after reload.
CSCus02258	ASA WebVPN: Cosmetic Syslog 734004 DAP: processing error: Code 2991
CSCus03141	ipsec-datapath:TFW management connection via VPN takes a few minutes
CSCus06165	ASA:Dataplane capture doesn't capture packets From Service module to ASA
CSCus06652	ASA5580-20 8.4.7.23: Traceback in Thread Name: ssh
CSCus08101	ASA: evaluation of Poodle Bites in TLSv1
CSCus09225	"sysopt traffic detailed-statistics" not visible in "show run"
CSCus11465	ASA teardown connection after receiving same direction fins
CSCus14147	ASA generate pool exhausted for sip inspect with embedded IP but no port
CSCus15721	ASA: ICMP loop when cluster member rejoins the cluster.
CSCus19673	"no nameif" is removing the policy-route configuration
CSCus23416	ASA traceback in DATAPATH-1-2414 after software upgrade
CSCus24519	ASA Cluster: Default OSPF route gone on Master unit

Identifier	Description
CSCus27696	ASA:- SSH un-authenticated connections are not timing out
CSCus29775	SSL: Sporadic TLS 1.2 connection errors on 5500-X platforms with DHE
CSCus30833	ASA: Page fault traceback in SXP CORE thread
CSCus34033	ASA fails to pass ipv6 address to anyconnect client when using RADIUS
CSCus39403	Cannot bootup ASA-V-KVM when deployed via RHEL/OpenStack
CSCus42901	JANUARY 2015 OpenSSL Vulnerabilities
CSCus46309	ASA : Failover descriptor does not change after reconfiguring VLAN
CSCus47192	NAT conversion fails when port range 1024 65535 is source
CSCus48874	genikev2: EAP with successful Authentication + Authorization may fail
CSCus49034	Tunnel default gateway no longer works in 9.3.2
CSCus49405	SCH enrollment issue with Saleen serial number
CSCus51289	ASA: Traceback when removing manual NAT rule
CSCus54537	ASAv requires a reboot for the license to take effect.
CSCus57241	ASA 9.3.2:DAP intermittently uses dflt policy for VPN RA sessions
CSCus64394	Misleading route-map warning message
CSCus69021	5506-X: 'no buffer' interface counter reports incorrect errors
CSCus71190	LDAP over SSL fails when using TLS1.2 on ASA
CSCus76060	ASA clears the TOS value of ICMP echo reply packet from ASA's interface
CSCus76632	assertion "mh->mh_mem_pool> MEMPOOL_UNDEFINED && mh->mh_mem_pool < MEMP
CSCus78109	Policy based routing is not working with twice NAT
CSCus79129	ASAv crashes when CiscoTAC-1 profile pointed to Transport Gateway w/ dbg
CSCus79307	ASAv cannot send SL messages after toggeling of "service call-home" cmd
CSCus83942	ASA : ACL logging is not getting disabled with keyword "log disable"
CSCus86487	PBR: DF & DSCP bits are not getting set without valid set next-hop
CSCus89139	Exception on asdm_handler stream line: </threat-detection>
CSCus89286	ASA Traceback in SSL library due to DMA memory exhaustion
CSCus94026	Cisco ASA ISAKMP Denial of Service Vulnerability

Identifier	Description
CSCus95290	Cisco ASA VPN XML Parser Denial of Service Vulnerability
CSCus98250	ASA WEBVPN: Usernames shown as '*' in logs for failed authentication
CSCut04996	DHCP Relay Server in interface mode not getting deleted
CSCut11895	Failover assembly remained in active-active state permanently
CSCut28210	AAA: RSA/SDI integration failing with ASA 9.3(2) - node secret issue
CSCut45114	2048-byte block leak if DNS server replies with "No such name"

End-User License Agreement

For information on the end-user license agreement, go to <http://www.cisco.com/go/warranty>.

Related Documentation

For additional information on the ASA, see [Navigating the Cisco ASA Series Documentation](#).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017 Cisco Systems, Inc. All rights reserved.