Release Notes for Cisco Service Control Operating System (SCOS) 3.1.5

OL-14438-06

These release notes for the Cisco Service Control Operating System describe the functional enhancements and fixes provided in Cisco Release SCOS 3.1.5. These release notes are updated as needed.

For information regarding features added and issues resolved in the 3.0.x train, please refer to *Release Notes for Cisco Service Control Operation System (SCOS) 3.0.6.*

For a list of the caveats that apply to Cisco Release SCOS 3.1.5 see Open Caveats, page 20.

Supports: SCOS 3.1.5, SCOS 3.1.1, and SCOS 3.1.0.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

SCOS 3.1.5 is a maintenance release of SCOS 3.1.0. It includes fixes of issues that were identified as part of Cisco's on going internal testing and during our interaction with our customers.

This document outlines the resolved issues delivered in the SCOS 3.1.5 release. It assumes the reader already has a good working knowledge of the Cisco Service Control solution. For additional information, please refer to the Cisco Service Control Engine documentation.

Note Cisco has been streamlining and improving its user interface. To access the new Cisco Service Control online documentation site, please do the following:

1. Go to the following page on Cisco.com: *http://www.cisco.com/web/psa/products/index.html*
2. From the **Select a category** list, select 'Service Exchange'.
3. From the **Select a sub-category** list, select the desired Cisco Service Control category.
4. From the **Select a product** list, select the desired Cisco Service Control product.

SCOS RELEASE 3.1.5

Compatibility Information

SCOS 3.1.5 may be installed on the following Service Control Engine platforms:

- SCE 2020 4xGBE
- SCE 2020 4/8xFE
- SCE 1010 2xGBE (2-U only)

SCOS 3.1.5 is not compatible with the following Service Control Engine platform:

- SCE 1010 2xGBE (1.5U)

Functional Enhancements

The following section lists the functional enhancements in SCOS release 3.1.5. See the either the *Cisco Service Control Engine Software Configuration Guide* or the *Cisco Service Control Application for Broadband User Guide* for more information regarding these features.

DSCP Marking Enhancements

SCOS release 3.1.5 decouples DSCP marking from the SCE platform queuing mechanism and provides a simplified GUI configuration for DSCP marking based on seven possible DSCP values. After an application is classified by the SCE, the DSCP-marking functionality can mark the relevant packets per package, service, and traffic direction.

Managing MPLS-VPN Branches

SCOS release 3.1.5 extends the functionality of managing an MPLS-VPN as a managed subscriber by supporting the ability to define a branch or site as the managed subscriber. The solution provides DPI usage analysis and control per branch of an enterprise in an MPLS-VPN encapsulation.

Identifying Subscribers per VLAN ID and IP

SCOS release 3.1.5 adds the ability to define a subscriber through a combination of VLAN ID and IP address range (subnet).

Flexible Subscriber Introduction

With the introduction of SCA BB release 3.1.5, the Radius Listener LEG component of the Subscriber Manager infrastructure can now leverage a Regular Expressions infrastructure for extracting and manipulating VSA attributes.

Backward Compatibility

MPLS L3-VPN

The 3.1.5 configuration supports a number of differet use cases. For more information, please consult the *Cisco Service Control Engine (SCE) Software Configuration Guide* and the *Cisco Service Control MPLS/VPN Solution Guide* .

DSCP Marking

The concept of mapping traffic portions to a specific DSCP value has changed in release 3.1.5. In previous versions of the SCA-BB solution, the mapping was only possible based on the CoS (Diffserv Class of Service) to which the Service was mapped. Starting with 3.1.5, it is possible to map each service to one of seven configurable DSCP values independently. The old DSCP marking mode is no longer supported.

Resolved Issues

The following issues were resolved in this release.

Upgrading the SM causes SCE failover in cascade topology

- Cisco Number CSCsi70273

  SCE platform performs failover procedure between active and standby SCE platforms in a cascaded pair when the connection to the SM goes down, even if no failover behavior is configured for this situation

  This issue is fixed in SCOS 3.1.5.

Non-first fragments misclassified

- Cisco Number Cisco Number CSCsk38279

  In very rare cases, non-first fragments were misclassified to a different flow and thus potentially dropped.

  This issue is fixed in SCOS 3.1.5.

'debug' command caused reboot with fatal error

- Cisco Number CSCsk94488

  ' **debug reset-to-default** ' command caused a reboot with a fatal error.

  This issue is fixed in SCOS 3.1.5.

ip ftp username and password did not work

- Cisco Number CSCsk06749

  The' **ip ftp username** ' and ' **ip ftp password** ' commands did not work properly in SCOS 3.1.0.

  This issue is fixed in SCOS 3.1.5.

Upgrading to PP#11 caused error

- Cisco Number CSCsk96368

  Upgrading to PP11 in both 3.1.0 and 3.1.1 resulted in error messages during and after protocol pack installation.

  The errors were similar to the following:

  ```
  T10/13/07 10:52:44 [000000171673:902:119] | 002 | 0000000721 | 0000000 | >
  [0x0a10:0x0004] System Message: Standard output/error message:
  Basic Host Context counter below zero!Basic Host Context counter below zero!Basic Host
  Context counter below zero!Basic Host Context counter below zero!Basic Host Context
  counter below zero!
  ```

  The messages had no impact on system behavior.

  The rate of the messages decreases with time - depending on the traffic, it may take several hours or days for the messages to stop appearing entirely

  This issue is fixed in SCOS 3.1.5.

Defining traffic rules not permitted at the admin authorization level

- Cisco Number CSCsj21478

  When the ‘ **traffic-rule** ’ command was executed from the admin authorization level, no traffic rule was created and the following error message appeared:

  Error - Required privilege level higher than current level.

  This issue is fixed in SCOS 3.1.5.

SCE platform should block simultaneous ‘get support-file’ commands from multiple interfaces

- Cisco Number CSCsk40370

  If a **"logger get support-file"** CLI command and a support file extraction operation via the SCA-BB console were executed simultaneously, both operations failed on timeout. Any subsequent support file extraction attempts failed as well.

  This issue is fixed in SCOS 3.1.5.

Could not add VLAN mapping to VPN after removing mapping when subscriber mappings are logged in (3.1.5LA)

- Cisco Number CSCsj98757

  When a VLAN mapping was removed from a VPN while subscriber mappings (IP@VPN) on the VPN were logged in, subsequent attempts to add a VLAN mapping to that VPN failed with an internal error.

  This issue is fixed in SCOS 3.1.5.

Misclassification in MPLS/VPN auto-learn mode

- Cisco Number CSCsj68557

  In MPLS/VPN auto-learn mode, misclassification and a high ratio of unidirectional flows occurred under certain traffic conditions. Warnings in the debug log from flow tunnel support and/or upstream labels aging were indicative of the problem.

  This issue is fixed in SCOS 3.1.5.

Using TIR in MPLS environment caused SCOS - CAM crash

- Cisco Number CSCsh90944

  Configuring a TIR with IP 0 caused the mechanism that classifies subscribers to TPs to crash.

  This issue is fixed in SCOS 3.1.5.

First subscriber had no expiration time (3.1.5LA)

- Cisco Number CSCsk10218

  The first subscriber logged in via SCE Lease Query LEG had no expiration time.

  This issue is fixed in SCOS 3.1.5.

RDRV1 destination startup configuration failed in downgrading from Release 3.1.0 to a previous release

- Cisco Number CSCsi96575

  When configuring RDR formatter RdrV1 destinations (even when using the old, backward-compatible command syntax), the running-config and hence the startup-config were updated with the new (as of 3.1.0) format of the command, which implicitly states the protocol and transport type. Due to this behavior, in a downgrade scenario, the startup configuration failed to configure the RDR formatter destination, since protocol and transport type are not supported. This resulted in losing reports.

  This issue is fixed in SCOS 3.1.5.

SCE-Sniffer RADIUS LEG did not work after PQI installation

- Cisco Number CSCse19753

  After installing a SCA BB PQI file on the SCE platform and before applying a service configuration for the first time, the SCE application ignored all open flows. When a service configuration is applied for the first time, the SCE application starts processing new flows. However, older flows that were opened earlier were not processed, and no RDRs were generated for them. RADIUS sniffing is susceptible to this limitation because it is likely that the relevant RADIUS flow would be open before the first time a service configuration is applied.

  This issue is fixed in SCOS 3.1.5.

Subscribers data synchronization was slower when static subscribers are configured

- Cisco Number CSCsi82338

  After the cascade links are up, the active box synchronizes the subscriber database to the standby box at a rate of ~1000 updates/sec. However the standby box could support this login rate only for dynamic subscribers. If there were static subscribers configured, it took up to an hour to synchronize the subscriber database after the cascade links were up. However, once the standby box was synchronized, new subscribers were replicated to the standby box normally (at a maximal delay of 2 minutes).

  This issue is fixed in SCOS 3.1.5.

CLI command 'IP address' did not indicate to the user that a reload of the SCE is required

- Cisco Number CSCsi56724

  After a change was made to the management IP/subnet, the SCE platform CLI should have output a message notifying the customer that a reload was required for the changes to take effect.

  This issue is fixed in SCOS 3.1.5.

TCP Learning did not close flows that started with SYN-ACK

- Cisco Number CSCsg85546

  In MPLS/VPN auto-learn mode, upstream SYN-ACK packets of unlearned labels reached the software even though they should not have.

  This issue is fixed in SCOS 3.1.5.

SCOS RELEASE 3.1.1

Compatibility Information

SCOS 3.1.1 may be installed on the following Service Control Engine platforms:

- SCE 2020 4xGBE
- SCE 2020 4/8xFE
- SCE 1010 2xGBE (2-U only)

SCOS 3.1.1 is not compatible with the following Service Control Engine platform:

- SCE 1010 2xGBE (1.5U)

Resolved Issues

The following issues were resolved in this release.

SCE reloads when over utilized with massive error dumps to log

- Cisco Number CSCsj48885

  The SCE can sometimes be forced to reload due to a watchdog expiry. This can occur under the following conditions:

  - The system is over utilized—CPU utilization at more than 75% and more then one million open HW flows
  - High error rate due to behavioral classification failures

- These conditions can cause massive error dumps to the log, triggering a timeout of the traverser watchdog. This in turn causes an invalid memory access, which results in a timeout of the system watchdog. It is the timeout of this system watchdog which causes the SCE platform reload.

  This issue is fixed in SCOS 3.1.1.

RADIUS/DHCP sniffer in SCE might stop functioning for certain flows

- Cisco Number CSCsi82268

  The SCE stops provisioning RADIUS transactions on certain flows. This can occur in the following situations:

  - Memory shortage—The SCE is working outside its capacity envelope (high probability).
  - RADIUS sniffer handler performs an illegal operation on the specific flow.

  This issue is fixed in SCOS 3.1.1.

SCE might reload in rare cases due to an infinite loop in its scheduler

- Cisco Number CSCsj32733

  If the target time for one of the traffic processor subtasks happened to coincide with the high resolution tick count wraparound, the SCE reloaded due to system watchdog.

  The user log message issued the following with no prior indication:

  ```
  "SE Watchdog Module: An Error occurred. Please report to Cisco's customer support"
  ```

  Debug log issued the following messages with no prior indication (RuC number may vary between 1-3):

  ```
  <<ERROR>> [0x0781:0x0013] Line Card Watchdog:  RuC number 1 timeout, keep alive timer
  = 500 milliseconds.
  <<ERROR>> [0x0781:0x0017] Line Card Watchdog:  Line card failed.
  ```

  This issue is fixed in SCOS 3.1.1.

Problem with fragments classification consumes log assets

- Cisco Number CSCsj05047

  In rare cases a log message of the following type may appear in the log:

  ```
  [0x0807:0x006c] FC: Total number of packets equals total number of non first fragments
  in flow counters
  ```

  This can cause the following issues:

  - Incorrect fragments classification—This is a sanity check which implies that the direction is not computed correctly for certain fragments
  - The log fills up since the dump message is large.

  This issue is fixed in SCOS 3.1.1.

Global-Controllers triggers warnings to the log when querying the MIB Group

- Cisco Number CSCsh99423

  When querying the global-controllers MIB group counters, the following warning is printed to the log for any global-controller index above 64 and for every port:

  ```
  <WARNING>[0x0b80:0x000e] SeMib: globalControllersEntry_lookup
  droppedCounters.actualNumberOfCounters=64 <= gcIndex=64 (port=1)!.
  <WARNING>[0x0b80:0x000e] SeMib: globalControllersEntry_lookup
  droppedCounters.actualNumberOfCounters=64 <= gcIndex=65 (port=1)!.
  .....
  <WARNING>[0x0b80:0x000e] SeMib: globalControllersEntry_lookup
  droppedCounters.actualNumberOfCounters=64 <= gcIndex=1023 (port=1)!.
  ```

  This issue is fixed in SCOS 3.1.1.

Bad response to a SNMP query and a Warning in DBG log

- Cisco Number CSCsi81920

  When performing a get operation on port number 2 (a management port in rev G), the following message is added to the debug log:

```
05/04/07  22:55:47 [000000125119:265:475] | 000 | 0000014556 | 0000000 |
<WARNING>[0x0b80:0x0011] SeMib: globalControllersEntry_lookup
CARDS_GetLimiterBandwidthCfg failed. Error is:interface number must be between 1 and 4
```

  This warning is generated each time the SNMP query is accepted and it means that the SCE responds to the SNMP query with a **gen_error** code, instead of either responding with a proper value, or responding with a **no_such_instance** error.

  This issue is fixed in SCOS 3.1.1.

SCOS RELEASE 3.1.0

New Features

Uni-directional classification for support of asymmetric routing

In a situation in which the routing scheme directs the two directions of a flow to follow different routes, each direction flows through a different SCE platform. The effect of different routing is that each SCE platform can classify only one direction of the flow. The ‘asymmetric routing’ mode enables the SCE platform to handle such traffic, allowing SCA BB to classify traffic based on a single direction and to apply basic reporting and global control features to uni-directional traffic.

See “Asymmetric Routing Topology” in Chapter 7, “Configuring the Connection” , in the *Cisco Service Control Engine Software Configuration Guide* , and the relevant topics in the *Cisco Service Control Application for Broadband User Guide*

NetFlow V9

Starting from Release 3.1.0 of SCOS for Cisco Service Control, the product can deliver gathered reporting data over the NetFlow V9 export protocol. This protocol is an industry standard for delivering gathered reporting data for external application for collecting, aggregation, storage, and processing. The NetFlow export protocol enables the Service Control solution to integrate with a wide range of existing data collectors and reporters.

See Chapter 8, “Raw Data Formatting: The RDR Formatter and NetFlow Exporting” in the *Cisco Service Control Engine Software Configuration Guide* .

Subscriber synchronization in cascade setups

SCOS 3.1.0 enhances support of failover in cascade topologies by adding a synchronization process between the active and the standby SCE platforms. This process keeps the standby SCE platform constantly updated with the latest subscriber-related information (login, logout, and quota updates), to minimize information loss if fail-over.

See the section “Synchronizing Subscriber Information in a Cascade System” in Chapter 9, "Managing Subscribers” in the *Cisco Service Control Engine Software Configuration Guide* .

Compatibility Information

SCOS 3.1.0 may be installed on the following Service Control Engine platforms:

- SCE 2020 4xGBE
- SCE 2020 4/8xFE
- SCE 1010 2xGBE (2-U only)

SCOS 3.1.0 is not compatible with the following Service Control Engine platform:

- SCE 1010 2xGBE (1.5U)

Resolved Issues

The following issues were resolved in this release.

SSH activity sometimes ended in an unstable state

- Cisco Number CSCsh49563

  During SSH activity, which usually includes session logout and login operations, the system sometimes ended in an unstable state due to file system violation.

  This issue is fixed in SCOS 3.1.0.

Redirect packet was sometimes transmitted on wrong link

- Cisco Number CSCsh74592

  When a flow using different links for upstream and downstream was redirected, the redirect packet to the subscriber was transmitted on the downstream link, but included the source MAC address from the GET packet seen on the upstream link as destination MAC address. This MAC address was sometimes unknown to the device receiving it.

  This issue is fixed in SCOS 3.1.0.

Dynamic Signature (DSS) caused a reboot after dozens of consecutive Apply operations

- Cisco Number CSCsi40164

  Applying a policy using DSS sometimes caused an infinite loop, resulting in a reboot of the SCE platform.

  This issue is fixed in SCOS 3.1.0.

Reload of the SCE due to an expiry of an internal watchdog mechanism

- Cisco Number CSCsi53483

  Under the following conditions, the SCE platform sometimes reloaded due to an expiry of an internal watchdog mechanism:

  – SCE platform working past its capacity envelope

  AND

  – The rate of the warning messages that BW controllers cannot be allocated is very high

  This issue is fixed in SCOS 3.1.0.

The saving process of application configuration was not resilient to reload

- Cisco Number CSCsi44806

  Running configuration of the application was not saved in cases of sudden reboots. In such cases, the SCE platform came up with no application configuration.

  This issue is fixed in SCOS 3.1.0.

Failure to retrieve support file using FTP

- Cisco Number CSCse63425

  An error occurred when attempting to retrieve a support file using FTP.

  The failure to retrieve the support file was caused by a timeout on the FTP server. When the SCE produces the support file (in zip format), it first produces the contents locally and then adds the contents to the zip file. When the support file is created over an FTP connection, there are long periods of no data transfer during the creation of the zip internal data. These long periods of no data transfer can trigger a connection timeout on the FTP server.

  This issue is fixed in SCOS 3.1.0.

PRPC authentication security level was set to default after RPC adapter restart

- Cisco Number CSCsh71764

  The PRPC connection to the SCE failed after restarting the PRPC server.

  This occurred when the security level was changed to something other than the default (semi) and the PRPC server was restarted. After the restart, the security level reverts back to the default value.

  This issue is fixed in SCOS 3.1.0.

Part of the quota information was not exchanged between two cascaded SCE platforms

- Cisco Number CSCsf97557

  Part of the quota information was not exchanged between two cascaded SCE platforms. This caused the failover in SCE cascade topology to be stateless with regard to quota.

  This issue is fixed in SCOS 3.1.0 (see Subscriber synchronization in cascade setups, page 12).

Subscriber with many mappings did not send all lease time expiration notifications

- Cisco Number CSCsg02338

  A subscriber with many mappings did not send lease time expiration notification on some mappings.

  This issue is fixed in SCOS 3.1.0

Link reflection failed to operate after long uptime

- Cisco Number CSCsh73979

  Link failure reflection sometimes failed to operate on a system with uptime of more than 24 days.

  This issue is fixed in SCOS 3.1.0.

Attack-detector port-list showed random numbers in running-config

- Cisco Number CSCsi11990

  When a port list was configured for an attack-detector, the specified ports were not saved correctly to the running-config. A list of random numbers was saved.

  This issue is fixed in SCOS 3.1.0.

Potential discard of packet under extreme network conditions

- Cisco Number CSCsi24848

  Under certain conditions, the Flow Filter rule used for congestion handling took effect a few mSec too late, allowing some packets to be discarded.

  This issue is fixed in SCOS 3.1.0.

Access violation when configuring anonymous groups

- Cisco Number CSCsg37325

  The following two scenarios sometimes caused an access violation:

  – Configure: `subscriber anonymous-group name sub1 IP-range 0.0.0.0/32` and transmit traffic. Then remove this group and wait for the flow to end.

    Then configure: `subscriber anonymous-group name sub1 IP-range 0.0.0.0/0` and transmit traffic.

  – Configure `anonymous-group name sub1 IP-range 0.0.0.0/32` and `anonymous-group name sub2 IP-range 0.0.0.0/0`

    Then remove sub1.

  This issue is fixed in SCOS 3.1.0.

destConnectionStatus of the rdr-formatter group was missing in 'show snmp MIB pcube-SE-MIB rdr-formatter' command

- Cisco Number CSCsf29452

  The MIB object *destConnectionStatus* of the rdr-formatter group was missing in CLI ' `show snmp MIB pcube-SE-MIB rdr-formatter` ' command.

  This issue is fixed in SCOS 3.1.0.

rdrActiveConnectionTrap was not sent after reload of the SCE platform

- Cisco Number CSCsg83522

  The proprietary trap ' *rdrActiveConnectionTrap* ', which should be sent after completing a successful establishment of a connection with the RDR collector, was not sent upon system initialization.

  This issue is fixed in SCOS 3.1.0.

Link up/down traps were not sent on all ports

- Cisco Number CSCsh31706

  The SNMP traps 'link up'/'link down', which should be sent for each port upon system initialization, were sent only on the first four ports of the SCE platform.

  This issue is fixed in SCOS 3.1.0.

MIB object 'pmoduleType' returned wrong value in cascade setups

- Cisco Number CSCsh34432

  The MIB object *pmoduleType* of PcubeSeMib returned the wrong value in cascade setups, indicating that there were only two GBE ports in the SCE platform.

  This issue is fixed in SCOS 3.1.0.

MIB variable ifMtu returned wrong value for traffic ports

- Cisco Number CSCsh99422

  The MIB-II variable *ifMtu* returned an incorrect value for the maximum packet size of the SCE platform traffic ports.

  This issue is fixed in SCOS 3.1.0.

Some rdr-formatter MIB objects returned information only for category 1

- Cisco Number CSCsi01850

  Global MIB objects in the *RdrFormatterGrp* in the PcubeSeMib should indicate total values for all categories of the RDR formatter. Previously these objects contained only the values for Category 1.

  This issue is fixed in SCOS 3.1.0.

Limitations and Restrictions

The upgrade to the SCOS 3.1.5 release may result in re-initialization of the SCE 1010 or SCE 2020 hardware Bypass module. This re-initialization process may cause a failure of the GBE link where the system stalls for a period of less than 1 sec.

The table below states the various cases when this re-initialization may occur (marked as "Yes").

Table 1 Possible Re-Initialization when Upgrading

To From	2.5.8	2.5.9	3.0.0	3.0.1	3.0.3	3.0.4	3.0.5	3.0.6	3.1.0	3.1.1	3.1.5
2.5.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.5	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.6	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.7	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.8	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.9	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3.0.0	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3.0.1	-	-	-	-	-	-	-	-	-		-
3.0.3	-	-	-	-	-	-	-	-	-	-	-
3.0.4	-	-	-	-	-	-	-	-	-	-	-
3.0.5	-	-	-	-	-	-	-	-	-	-	-
3.0.6	-	-	-	-	-	-	-	-	-	-	-
3.1.0	-	-	-	-	-	-	-	-	-	-	-
3.1.1	-	-	-	-	-	-	-	-	-	-	-

The SCE platform may experience a reboot when a port scan operation is performed on the SCE platform management port. This reboot is initiated by the SCE platform due to scheduling optimization for detecting failover conditions in periods of less than 1 second in a configuration of two cascaded SCE platforms.

The following is recommended:

- Use IP access lists to eliminate port scans that take place due to actual attacks.
- If the system administrator needs to perform a port scan operation as part of a security check, it is advisable to disable the SCE watchdog only for the period of time in which the port scan is performed.

  Use the following root-level CLI commands to disable the SCE watchdog:

```
configure
watchdog software-reset disabled
interface linecard 0
no watchdog
```

Use the following root-level CLI commands to re-enable the SCE watchdog:

```
configure
watchdog software-reset enabled
interface linecard 0
watchdog
```

Open Caveats

Rel 3.0.3: Invalid injected packet in MPLS traffic engineering mode

- Cisco Number CSCsl22211

  When working in ' **MPLS Traffic-Engineering skip** ' mode, a malformed packet is generated by the SCE when MPLS flows are redirected or blocked. In the injected packet, the 'next protocol' field of the Ethernet header is 0x8847 (MPLS), but should be 0x0800 (IPv4).

  Workaround: Configure the system to ‘*MPLS VPN skip*’.

  This has a performance penalty, but in this mode the system injects properly formed packets.

DSCP marking+inject+tunneled traffic generates malformed injected packet

- Cisco Number CSCsl41385

  When working in tos-marking mode and the application injects over tunneled traffic (VLAN/MPLS), the injected packets are malformed since the ToS is updated at the wrong offset in the packet. The results of this are:

  - In MPLS and VLAN the labels/vlan-id are wrong.
  - The IP header checksum is incorrect.
  - The packets are marked as mid-fragments in the IP header

While removing all VPNs management operations cannot be performed

- Cisco Number CSCsj85601

When removing all VPNs from the SM using the " **--force** " option, some management operations cannot be performed on the SCE until the operation completes. This occurs only when removing many VPNs that have active subscriber mappings in the SCE.

Workaround: Instead of removing the VPNs along with their subscriber mappings by using the **--force** option, remove the subscribers first, and only then remove the VPNs (without the **--force** option.

Tunnel-id-based traffic rule applies DSCP marking to non-tunneled traffic

- Cisco Number CSCsj32282

  A tunnel-id-based traffic rule defining DSCP marking applies the DSCP marking to non-tunneled traffic, also.

  Workaround: When defining the traffic rule, always set the URG flag. For existing rules, replace with a new rule that is identical, with the addition of setting the URG flag.

SCE2000 may reload if stalled by flow control

- Cisco Number CSCsi80337

  By design, the SCE platform reacts to Ethernet flow control and doesn't activate it. Therefore, it is possible for a situation to arise in which flow control stalls the SCE platform by overflowing the SCE platform queues and thereby causing traffic to be dropped on the Rx interfaces. If this situation persists for more than five seconds, it may trigger the SCE platform internal sanity checks mechanism, which may in turn trigger a reload of the SCE platform in an attempt to recover.

SCE2000 may drop cascade control packets from AF4 queue during GC congestion

- Cisco Number CSCsj93315

  Extra care must be given to the configuration of the link shapers in 'inline-cascade' connection mode. Configuring the shaper in an aggressive manner might result in very high rate of tail-dropped packets. In extreme situations, packets that are used for the High Availability protocol monitoring and control may be dropped. Thus, an extreme situation could result in false detection of a failure and an unnecessary switchover between the active and standby SCE platforms

'no service telnetd' command does not block the Telnet port

- Cisco Number CSCsh21957

  Disabling the Telnet server of the SCE (using the CLI command 'no service telnetd') disables any new Telnet connection to the SCE platform, but does not block the Telnet port.

  Workaround: There is no workaround that will enable blocking this specific service at a lower level.

Use the '`ip access-class`' command to restrict access to the SCE platform at the IP level. Configuring the SCE platform to deny a certain IP address would prevent communication with that address using any IP-based protocol, including Telnet, FTP, ICMP and SNMP. The basic IP interface is low-level, blocking the IP packets before they reach the higher level services

Vulnerability to malicious SSH activity or abuse of SSH

- Cisco Number CSCsi68582

  The SCE platform suffers from vulnerability to malicious SSH activity or abuse of SSH, which may result in reboot or system unavailability.

  Workaround

  - Use ACL to restrict access to the SCE over the management interfaces.
  - Disable the SSH server and use Telnet instead, where these vulnerabilities do not exist.

Link failure may be reflected to all ports if a port is flickering due to a HW problem

- Cisco Number CSCsg46885

  When link reflection on all ports with linecard aware is configured, the link failure may be reflected to all ports (rather than only to the relevant link) if one of the ports that is connected to the failed linecard is flickering due to a hardware problem.

TCP Learning doesn't close flows that start with SYN-ACK

- Cisco Number CSCsg85546

  In MPLS/VPN auto-learn mode, upstream SYN-ACK packets of unlearned labels reach the software even though they should not.

  This is relevant mainly when using anonymous subscribers with a range that contains addresses that appear in one of the VPNs. In this case, anonymous subscribers may be incorrectly spawned for addresses inside VPNs. Such subscribers see very little, if any traffic.

Potential memory overrun in cascaded environment with a high number of subscribers

- Cisco Number: CSCsc96282

  Under rare conditions, the standby SCE platform of a cascaded pair crashes and restarts. This may happen in a scenario involving a heavy load of anonymous subscribers in cascade topology.

  In such a case, only the standby box is affected, and therefore:

  - overall service is not compromised
  - fault tolerance is compromised only for the time it takes the standby box to restart.

The configured attack threshold is set for each PPC separately

- Cisco Number: CSCsd48922

  For certain types of attacks, an attack is detected by the SCOS attack-filter module only if it is three times stronger (as measured by flow rate per second) than the configured value.

  This happens when the IP address common to all the flows of the attack is on the network side of the SCE platform, so all attacks of type 'single-side-network' have this problem

When the VAS Health Check initializes, the CLI command 'show interface linecard 0 VAS-traffic-forwarding VAS server-id <id>' shows the server being UP even if it is actually Down

- Cisco Number CSCse05325

  The operative state of a VAS server while the Health Check is in Init state is considered to be Up as shown in the CLI command "`show interface linecard 0 VAS-traffic-forwarding VAS server-id <id>`". In addition, during this time, the SCE platform may forward VAS traffic to this server.

Flow 'opened from VAS' is misrouted if there is a FF rule to bypass

- Cisco Number CSCsc49573

  When VAS mode is enabled, the system generally assumes that traffic with a VLAN tag is VAS traffic coming from the VAS servers, and therefore forwards it to the non-VAS link.

  However, under the following conditions, a flow will be forwarded by the SCE platform on the same link on which it was received and with no VLAN tag:

  - VAS mode is enabled
  - The FIF packet has a VLAN tag
  - There is a traffic rule to bypass the flow or the SCE platform is in congestion

  In some topologies this behavior may cause VAS traffic to be incorrectly routed back to the VAS link.

Packet Loss during Application Installation or Upgrade

- Cisco Number CSCpu11798

  When a PQI application file is installed or upgraded on the SCE, the SCE may lose a few packets for a few seconds. The overall percentage of this phenomenon is very low.

  Workaround: It is advised to perform the upgrade in non peak time.

‘show snmp MIB pcube-SE-MIB port’ returns wrong number of ports

- Cisco Number CSCsg45606

  The CLI command ‘`show snmp MIB pcube-SE-MIB port `' returns the wrong number of ports, because Mng port 2 is treated as traffic port instead of 2nd management port.

  Workaround: Use SNMP browser rather than CLI command.

Obtaining Technical Assistance

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at any time, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com , you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to http://www.cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website http://www.cisco.com/tac.

P3 and P4 level problems are defined as follows:

- P3—Your network is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to http://tools.cisco.com/RPF/register/register.do.

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at http://www.cisco.com/tac/caseopen.

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.