Rev. A00
July 2020

DELL EMC

Dell S4810 System Release Notes, OS Version 9.14(1.9P4)

This document contains information on open and resolved caveats, and operational information specific to the Dell Networking OS software and the S4810 platform.
Current Version: 9.14(1.9P4)
Release Date: 2020-07-30
Previous Version: 9.14(1.8)

Topics:

Caveats are unexpected or incorrect behavior, and are listed in order of Problem Report (PR) number within the appropriate sections.

NOTE: Customers can subscribe to caveat update reports or use the BugTrack search tool to read current information about open and closed software caveats. To subscribe or use BugTrack, visit iSupport at: https://www.force10networks.com/CSPortal20/BugTrack/SearchIssues.aspx. BugTrack currently tracks software caveats opened in Dell Networking OS version 6.2.1.1 and later. All Release Notes are available on the Software Center tab of iSupport. The link to the relevant Release Notes for each software version is next to the link for that version: https://www.force10networks.com/CSPortal20/Software/Downloads.aspx.

For more information on hardware and software features, commands, and capabilities, refer to the Dell Networking support website at: https://www.dell.com/support

Document Revision History

Table 1. Revision History

Date	Description
2020–07	Initial release.

Supported Brocade Cables

The following Brocade cables are supported with this platform:

Table 2. Supported Brocade Cables

Cable Description
CUS,PCT B-8000 10GbE TWINAX 3 METER 8PACK
CUS,PCT B-8000 10GbE TWINAX 5 METER 1PACK
CUS,PCT B-8000 10GbE TWINAX 5 METER 8PACK
CUS,PCT B-8000 10GbE TWINAX 1 METER 1PACK
CUS,PCT B-8000 10GbE TWINAX 1 METER 8PACK
CUS,PCT B-8000 10GbE TWINAX 3 METER 1PACK

Supported Hardware

The following hardware is supported with this platform:

Table 3. Supported Hardware

Hardware
48 port 10G SFP+ ports with 4 QSFP+ 40G ports
48 port 10G SFP+ ports with 4 QSFP+ 40G ports, 1 DC power supply and 2 fan subsystem with airflow from I/O side to power supply unit (PSU) side
48 port 10G SFP+ ports with 4 QSFP+ 40G ports, 1 AC power supply and 2 fan subsystem with airflow from I/O side to power supply unit (PSU) side
48 port 10G SFP+ ports with 4 QSFP+ 40G ports, 1 DC power supply and 2 fan subsystem with airflow from power supply unit (PSU) side to I/O side
48 port 10G SFP+ ports with 4 QSFP+ 40G ports, 1 AC power supply and 2 fan subsystem with airflow from power supply unit (PSU) side to I/O side
S4810 Series – Fan with airflow from I/O side to power supply unit (PSU) side
S4810 Series – Fan with airflow from PSU side to I/O side
S4810 Series – DC Power supply with airflow from I/O side to power supply unit (PSU) side
S4810 Series – DC power supply with airflow from power supply unit (PSU) side to I/O side
S4810 Series – AC Power supply with airflow from I/O side to power supply unit (PSU) side
S4810 Series – AC Power supply with airflow from power supply unit (PSU) side to I/O side

NOTE: Fan Modules and Power supplies (PSUs) are field replaceable units. Dell Networking does not support a mix of power supply types (i.e., AC and DC) in the same switch.

NOTE: All fans and PSUs must have the same airflow direction. Should a mixed airflow configuration happen, the switch detects the discrepancy and performs a shutdown, if the module is not replaced within few minutes.

NOTE: Due to hardware limitation, 1G Cu SFP with QSA is not supported.

New Dell Networking OS Version 9.14(1.9P4) Features

The following features have been added to the S4810 with Dell Networking OS version 9.14(1.9P4):

None.

Restrictions

If an Intel X520 CNA adapter is used as an FCoE initiator, follow these steps to establish FCoE sessions to send and receive traffic on an S4810 switch:

1. On the server, uninstall the old Intel driver (version 13.0.0 or older).
2. Re-install the Intel driver using version 13.5 A00 (or later) from the http://www.dell.com website.Important: During the installation, do not select the ISCSI part of the driver; select only the FCoE check box.
3. On each server-facing port, enter the following commands in interface configuration mode. The dcbx version cee command configures a port to use the CEE (Intel 1.01) version of DCBX. Configure server-facing ports with the shutdown and no shutdown commands as needed. For example:

   ```
   Dell# interface tenGigabitEthernet 0/1
   Dell(conf-if-te-0/1)# portmode hybrid
   Dell(conf-if-te-0/1)# switchport
   Dell(conf-if-te-0/1)# protocol lldp
   Dell(conf-lldp)# dcbx port-role auto-downstream
   Dell(conf-lldp)# dcbx version cee
   Dell(conf-lldp)# exit
   Dell(conf-if-te-0/1)# spanning-tree pvst edge-port
   Dell(conf-if-te-0/1)# no shutdown
   Dell(conf-if-te-0/1)# exit
   Dell#
   ```

4. Display information on FIP-snooped sessions and check the entries in ENode Interface fields to see if you have established the FCoE session on a server-facing port.

   `show fip-snooping sessions`

   EXEC Privilege

- The following features are not available in the Dell Networking OS from version 9.7(0.0):
  - PIM ECMP
  - Static IGMP join (`ip igmp static-group`)
  - IGMP querier timeout configuration (`ip igmp querier-timeout`)
  - IGMP group join limit (`ip igmp group join-limit`)
- If you use the `interface range` command to select multiple interfaces that are added to the management VRF, the `ipv6 address` command does not display the `autoconfig` option. You can configure the `autoconfig` command on individual interfaces.
- If you use the `interface range` command to select multiple interfaces that are added to the management VRF, the `ipv6 nd` command displays the following options but they do not take effect if you use them:
  - dns-server
  - hop-limit
  - managed-config-flag
  - max-ra-interval
  - mtu
  - other-config-flag
  - prefix
  - ra-guard
  - ra-lifetime
  - reachable-time
  - retrans-timer
  - suppress-ra

Changes to Default Behavior and CLI Syntax

Following default behavior and CLI syntax changes occurred during the Dell EMC Networking OS release 9.14(1.9P4):

None.

S4810 Upgrade Procedures: Overview

To upgrade the Dell Networking OS to the latest version on a S4810 switch, complete these steps:

- Upgrading the S4810 Dell Networking OS Image and Boot Code
- Upgrading the CPLD
- VLT Upgrade Procedure

Upgrading the S4810 Dell Networking OS Image and Boot Code

The S4810 system is pre-loaded with default Dell Networking OS software.

NOTE: Before upgrading Dell Networking OS on S4810 from a version prior to 8.3.12.0 to version 9.14(1.9P4), ensure to increase the partition size by upgrading to version 8.3.12.0.

NOTE: If the upgrade image is greater than 32MB in size, switches running Dell Networking OS version prior to 9.1(0.0) do not support software upgrade using TFTP. Use FTP, SCP, FLASH, or NFSMOUNT instead. Dell Networking OS Version 9.1(0.0) introduced TFTP enhancements to support file transfers larger than 32MB.

NOTE: If VLT configurations exist on a switch that runs Dell Networking OS version 9.2(0.0) or prior, ensure that all switches in the VLT domain are upgraded to version 9.3(0.0) before upgrading to version 9.14(1.9P4).

NOTE: You can directly upgrade a switch that runs Dell Networking OS version 8.3.12.0 (or later) to version 9.14(1.9P4), if VLT configurations do not exist on that switch.

Bare Metal Provisioning

NOTE: If you are using Bare Metal Provisioning (BMP), refer to the Bare Metal Provisioning chapter in the Dell Networking OS Configuration Guide or the Open Automation Guide.

Manual Upgrade Procedure

Follow these steps to upgrade your S4810 system:

1. Dell Networking recommends that you back up your startup configuration and any important files and directories to an external media prior to upgrading the system.
2. Upgrade the Dell Networking OS in flash partition A: or B:

   `upgrade system [flash: | ftp: | scp: | tftp:] [A: | B:]`

   EXEC Privilege

   ```
   Dell#upgrade system ftp: a:
   Address or name of remote host []: 10.16.127.35
   Source file name []: FTOS-SE-9.14.1.9P4.bin
   User name to login remote host: ftpuser
   Password to login remote host:
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   Erasing Sseries Primary Image, please wait
   ............................................................................................
   ........................................................................................Wri
   ting .......................................................................................
   ...................................................................
   44220292 bytes successfully copied
   System image upgrade completed successfully.
   Dell #
   ```

3. In case of a stack setup, upgrade the Dell Networking OS for the stacked units.

   `upgrade system stack-unit [0-11 | all] [A: | B:]`

   EXEC Privilege

If A: is specified in the command, the Dell Networking OS version present in Management unit's A: partition will be pushed to the stack units. If B: is specified in the command, the Management unit's B: will be pushed to the stack units. Upgrade of stack units can be done on individual units by specifying the unit id [0-11] or on all units by using all in the command.

```
Dell#upgrade system stack-unit all A:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image upgraded to all
Dell#
```

4. Verify the Dell Networking OS has been upgraded correctly in the upgraded flash partition

   `show boot system stack-unit [0-11 | all]`

   EXEC PRIVILEGE

   The Dell Networking OS versions present in A: and B: can be viewed for individual units by specifying the stack unit id [0-11] in the command or for all the stack units by specifying all in the command.

```
Dell#show boot system stack-unit all

Current system image information in the system:
===========================================================
Type                        Boot Type       A                       B
-----------------------------------------------------------
Stack-unit 0                  FLASH BOOT    9.14(1.9P4)[boot]    9.14(1.8)
Stack-unit 1                  FLASH BOOT    9.14(1.9P4)[boot]    9.14(1.8)
Stack-unit 2 is not present.
Stack-unit 3 is not present.
Stack-unit 4 is not present.
Stack-unit 5 is not present.
Stack-unit 6 is not present.
Stack-unit 7 is not present.
Stack-unit 8 is not present.
Stack-unit 9 is not present.
Stack-unit 10 is not present.
Stack-unit 11 is not present.
Dell#
```

5. Upgrade the S4810 Boot Code.

   `upgrade boot [flash: | ftp: | scp: | tftp:]`

   EXEC Privilege

   Dell Networking OS version 9.14(1.9P4) requires S4810 Boot Code version 1.2.0.5. If any higher versions of Boot Code are present in the unit, do not upgrade the Boot Code.

```
Dell#upgrade boot ftp:
Address or name of remote host []: 10.16.127.35
Source file name []: U-boot.1.2.0.5.bin
User name to login remote host: ftpuser
Password to login remote host:
!
Erasing SSeries BootImageUpgrade Table of Contents, please wait
.!........Writing .................................!
524528 bytes successfully copied
Dell#
```

6. In case of a stack setup, upgrade the S4810 Boot Code to the stack units.

   `upgrade boot stack-unit [0-11 | all]`

   EXEC Privilege

   The S4810 Boot Code can be upgraded to individual units by specifying the stack unit ID [0-11] in the command or it can be upgraded on all stack units by specifying all in the command.

```
Dell#upgrade boot stack-unit all
!!!!!!!!!!
Dell#
```

7. Change the Primary Boot Parameter of the S4810 to the upgraded partition A: or B:

   `boot system stack-unit [0-11 | all] primary [system A: | system B: | tftp://URL]`

CONFIGURATION

8. Save the configuration so that the configuration will be retained after a reload using write memory command.

   `write memory`

   EXEC PRIVILEGE

   In case of a stack setup, the configuration will be saved in the Management as well as the Standby units.

   ```
   Dell#write memory
   !
   Synchronizing data to peer Stack-unit
   !!!!!!!!
   Dell#
   ```

9. Reload the unit

   `reload`

   EXEC PRIVILEGE

   ```
   Dell#reload

   Proceed with reload [confirm yes/no]: yes
   Jul 24 21:32:27: %STKUNIT0-M:CP %CHMGR-5-RELOAD: User request to reload the chassis
   syncing disks... done
   ```

10. Verify the S4810 has been upgraded to the Dell Networking OS version 9.14(1.9P4).

    `show version`

    EXEC PRIVILEGE

    ```
    Dell#show version
    Dell Real Time Operating System Software
    Dell Operating System Version:  2.0
    Dell Application Software Version:  9.14(1.9P4)
    Copyright (c) 1999-2019 by Dell Inc. All Rights Reserved.
    Build Time: Fri Jul 24 16:58:02 2020
    Build Path: /build/build02/SW/SRC
    Dell Networking OS uptime is 2 minute(s)

    System image file is "system://A"

    System Type: S4810
    Control Processor: Freescale QorIQ P2020 with 2 Gbytes (2147483648 bytes) of memory,
    core(s) 1.

    128M bytes of boot flash memory.

      1 52-port GE/TE/FG (SE)
     48 Ten GigabitEthernet/IEEE 802.3 interface(s)
      4 Forty GigabitEthernet/IEEE 802.3 interface(s)
    Dell#
    ```

11. Verify the S4810 has been upgraded to the latest Boot Code

    `show system stack-unit [0-11]`

    EXEC PRIVILEGE

    ```
    Dell#show system stack-unit 0

    --  Unit 0 --
    Unit Type                  : Management Unit
    Status                     : online
    Next Boot                  : online
    Required Type              : S4810 - 52-port GE/TE/FG (SE)
    Current Type               : S4810 - 52-port GE/TE/FG (SE)
    Master priority            : 0
    Hardware Rev               : 3.0
    Num Ports                  : 64
    Up Time                    : 2 min
    Dell Networking OS Version : 9.14(1.9P4)
    Jumbo Capable              : yes
    POE Capable                : no
    ```

```
FIPS Mode                  : disabled
Boot Flash                 : 1.2.0.5
```

SSH — SSH host keys are stored in NVRAM. Dell Networking OS regenerates them when Dell Networking OS applies the startup-config and the `ip ssh server enable` configuration. However, if the SSH client has “Strict Host Key” checking enabled, the SSH client denies access to the Dell Networking OS SSH server. To resolve this issue, you must modify the SSH client settings so that it uses the new key.

Upgrading the CPLD

The S4810 system with Dell Networking OS version 9.14(1.9P4) requires CPLD image 7.

Verify that a CPLD upgrade is required

Use the following command to identify the CPLD version loaded in the device:

```
Dell#show revision
--  Stack unit 0  --
S4810 SYSTEM CPLD       : 7
NPU PCI DEVICE ID       : 0xB845 (TRIDENT)

--  Stack unit 1  --
S4810 SYSTEM CPLD       : 7
NPU PCI DEVICE ID       : 0xB845 (TRIDENT)

--  Stack unit 2  --
S4810 SYSTEM CPLD       : 7
NPU PCI DEVICE ID       : 0xB845 (TRIDENT)

Dell#
```

Use the following command to view CPLD version that is associated with the Dell Networking OS image:

```
Dell#show os-version

RELEASE IMAGE INFORMATION :
-------------------------------------------------------------------------
      Platform          Version        Size           ReleaseTime
S-Series:  SE         9.14(1.9P4)           44220292       Jul 24 2020 17:24:13


TARGET IMAGE INFORMATION :
-------------------------------------------------------------------------
        Type          Version       Target                               checksum
     runtime         9.14(1.9P4)          Control Processor       passed

CPLD IMAGE INFORMATION :
-------------------------------------------------------------------------
         Card                      CPLD Name    Version
Stack-unit 0              S4810 SYSTEM CPLD          7
Stack-unit 1              S4810 SYSTEM CPLD          7
Stack-unit 2              S4810 SYSTEM CPLD          7
```

Upgrading the CPLD Image

NOTE: The upgrade fpga-image stack-unit {0-11} booted command is hidden when using the FPGA Upgrade feature in the CLI. However, it is a supported command and will be accepted when entered as documented.

To upgrade the CPLD image on the S4810:

1. Upgrade the CPLD image.

   ```
   upgrade fpga-image stack-unit [0-11] booted
   ```

EXEC Privilege

```
Dell# upgrade fpga-image stack-unit 0 booted

Current information for the system:
========================================================================
  Card                      Device Name    Current Version     New Version
------------------------------------------------------------------------
 Unit0                S4810 SYSTEM CPLD                  7               7

    ***********************************************************************
    *  Warning - Upgrading FPGA is inherently risky and should            *
    *  only be attempted when necessary.  A failure at this upgrade may   *
    *  cause a board RMA.  Proceed with caution !                         *
    ***********************************************************************

Upgrade image for stack-unit 0 [yes/no]: yes


FPGA upgrade in progress!!! Please do NOT power off the unit!!!
!!Jul 24 16:06:40: %S4810:0 %DOWNLOAD-6-FPGA_UPGRADE: stack-unit 0 fpga upgrade success.


Upgrade result :
================
Unit 0 FPGA upgrade successful Unit 0. will go for reboot to complete the upgrade.
Dell#
```

2. Check whether the CPLD has been upgraded to the latest version.

   `show revision`

   EXEC PRIVILEGE

```
Dell#show revision

--  Stack unit 0  --
S4810 SYSTEM CPLD        : 7
NPU PCI DEVICE ID        : 0xB845 (TRIDENT)

--  Stack unit 1  --
S4810 SYSTEM CPLD        : 7
NPU PCI DEVICE ID        : 0xB845 (TRIDENT)

--  Stack unit 2  --
S4810 SYSTEM CPLD        : 7
NPU PCI DEVICE ID        : 0xB845 (TRIDENT)
Dell#
```

VLT Upgrade Procedure

To upgrade the Dell Networking OS in a VLT setup from version 9.2(0.0) to the latest version, upgrade Dell Networking OS to version 9.3(0.0) first and then to the newer version. If you are already running Dell Networking OS version 9.3(0.0) or later, you can directly upgrade the Dell Networking OS to the latest version. To upgrade the Dell Networking OS, on systems running VLT, perform the following steps:

1. Upgrade the system-flash partition A or B with the new image on both VLT peers.On both the VLT peers, set Primary boot parameter to boot the system from upgraded system flash partition [A or B].You can enter one of the following options:**flash** — Copies from flash file system (flash://filepath).**ftp** — Copies from remote file system (ftp://userid:password@hostip//filepath).**scp** — Copies from remote file system (scp://userid:password@hostip//filepath).**tftp** — Copies from remote file system (tftp://hostip/filepath).

   `upgrade system [flash: | ftp: | scp: | tftp: | usbflash:] [A: | B:]`

   EXEC Privilege
2. Reload or power-cycle one of the VLT peers (For Example, Peer 2).

   `reload or power cycle`
3. Wait for Peer 2 to come up; VLT adjacency will be established. (Peer 2 - new image and Peer 1 - old image).

ⓘ **NOTE: Between software versions 8.3.10.0 & 9.4P1 both VLT peers are running different VLT versions, a VLT peering will not established.**

4. Wait for the Peer 2 to bring up all VLT LAG ports. Use the command `show vlt detail` to confirm all VLT ports in the local chassis are active.

   ```
   show vlt detail
   ```

   EXEC Privilege
5. Following upgrade, use the `write memory` command to save the running-config to memory.

   ```
   write memory
   ```

   EXEC Privilege
6. Ensure both the nodes are now forwarding traffic.

   ⓘ **NOTE:**

   - **When you upgrade VLT nodes from 8.3.12, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, and 9.10 to 9.14(1.9P4), forwarding traffic is not affected.**
   - **If you upgrade VLT nodes from 8.3.10.0 to 9.x.x.x, layer 2 switched packets are flooded until all MAC addresses are learned. Layer 3 routed packets are dropped until all ARP entries are resolved and routes are learned due to version mismatch.**

   Layer 2 switched packets will be flooded until all MACs are learned and Layer 3 routed packets will be dropped until all ARPs are resolved and routes are learned due to version mismatch.
7. When all VLT ports are active on the Peer 2, repeat steps 2 through 5 for the Peer 1.

   ⓘ **NOTE: After upgrading to the latest Dell Networking OS version, upgrade the CPLD if required.**

Documentation Corrections

This section describes the errors identified in the current release of the Dell Networking OS.

None.

Deferred Issues

Issues that appear in this section were reported in Dell Networking OS version 9.14(1.0) as open, but have since been deferred. Deferred caveats are those that are found to be invalid, not reproducible, or not scheduled for resolution.

Deferred S4810 9.14(1.0) Software Issues

Issues that appear in this section were reported in Dell Networking OS version 9.14(1.0) as open, but have since been deferred. Deferred caveats are those that are found to be invalid, not reproducible, or not scheduled for resolution.

The following issues have been deferred in the Dell Networking OS version 9.14(1.0):

None.

Fixed Issues

Fixed issues are reported using the following definitions.

Category	Description
PR#	Problem Report number that identifies the issue.
Severity	**S1** — Crash: A software crash occurs in the kernel or a running process that requires a restart of AFM, the router, switch, or process. **S2** — Critical: An issue that renders the system or a major feature unusable, which can have a pervasive impact on the system or network, and for which there is no work-around acceptable to the customer.

Category	Description
	S3 — Major: An issue that affects the functionality of a major feature or negatively effects the network for which there exists a work-around that is acceptable to the customer.
	S4 — Minor: A cosmetic issue or an issue in a minor feature with little or no network impact for which there might be a work-around.
Synopsis	Synopsis is the title or short description of the issue.
Release Notes	Release Notes description contains more detailed information about the issue.
Work around	Work around describes a mechanism for circumventing, avoiding, or recovering from the issue. It might not be a permanent solution. Issues listed in the “Closed Caveats” section should not be present, and the work-around is unnecessary, as the version of code for which this release note is documented has resolved the caveat.

Fixed S4810 9.14(1.9P4) Software Issues

NOTE: Dell Networking OS 9.14(1.9P4) includes fixes for caveats addressed in the previous 9.14 releases. Refer to the respective release notes documentation for the list of caveats fixed in the earlier 9.14 releases.

The following caveats are fixed in Dell Networking OS version 9.14(1.9P4):

PR# 169564	
Severity:	Sev 3
Synopsis:	The security vulnerability reported indicates that the DH512 private key is vulnerable. This is being used by OpenSSL library for secured communications like SSH and HTTPS applications (CVE-2019-1551).
Release Notes:	There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API `BN_mod_exp` may be affected if they use `BN_FLG_CONSTTIME`. Fixed in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u (Affected 1.0.2-1.0.2t), (CVE-2019-1551).
Workaround:	None
PR# 169623	
Severity:	Sev 3
Synopsis:	SHA1 is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks (CVE-2005-4900).
Release Notes:	SHA1 is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks (CVE-2005-4900).
Workaround:	Configure SHA256 instead of SHA1.
PR# 169691	
Severity:	Sev 3
Synopsis:	ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts (CVE-1999-0524).

Release Notes: ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts (CVE-1999-0524).

Workaround: None

PR# 169702

Severity: Sev 2

Synopsis: OpenSSH version 8.2p1, bundled with 9.14.2.7 and 9.14.1.9P4 or higher, fixes SHA-1 vulnerabilities.

Release Notes: OpenSSH version 8.2p1, bundled with 9.14.2.7 and 9.14.1.9P4 or higher, fixes SHA-1 vulnerabilities.

Workaround: None

PR# 169733

Severity: Sev 2

Synopsis: ntpd prior to 4.2.8p14 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address.

Release Notes: ntpd prior to 4.2.8p14 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp (CVE-2020-11868).

Workaround: None

PR# 169749

Severity: Sev 2

Synopsis: The switch becomes unresponsive due to a kernel memory leak when soft-forwarding multicast data.

Release Notes: The switch becomes unresponsive due to a kernel memory leak when soft-forwarding multicast data.

Workaround: None

PR# 169806

Severity: Sev 2

Synopsis: The login password displays as clear text in the RADIUS log when the RADIUS server is unreachable.

Release Notes: The login password displays as clear text in the RADIUS log when the RADIUS server is unreachable.

Workaround: None

PR# 169814

Severity: Sev 2

Synopsis: Processing a wrongly crafted router advertisement packet leads to a software exception.

Release Notes: Processing a wrongly crafted router advertisement packet leads to a software exception.

Workaround:	None

Known Issues

Known issues are reported using the following definitions.

Category	Description
PR#	Problem Report number that identifies the issue.
Severity	**S1** — Crash: A software crash occurs in the kernel or a running process that requires a restart of AFM, the router, switch, or process. **S2** — Critical: An issue that renders the system or a major feature unusable, which can have a pervasive impact on the system or network, and for which there is no work-around acceptable to the customer. **S3** — Major: An issue that affects the functionality of a major feature or negatively effects the network for which there exists a work-around that is acceptable to the customer. **S4** — Minor: A cosmetic issue or an issue in a minor feature with little or no network impact for which there might be a work-around.
Synopsis	Synopsis is the title or short description of the issue.
Release Notes	Release Notes description contains more detailed information about the issue.
Work around	Work around describes a mechanism for circumventing, avoiding, or recovering from the issue. It might not be a permanent solution. Issues listed in the “Closed Caveats” section should not be present, and the work-around is unnecessary, as the version of code for which this release note is documented has resolved the caveat.

Known S4810 9.14(1.9P4) Software Issues

The latest information related to Open Caveats is available on iSupport through the BugTrack search tool. BugTrack currently tracks software caveats opened in Dell Networking OS version 6.2.1.1 and later.

NOTE: **You must have a user account to access the BugTrack tool.**

To use the search tool:

1. Go the Main Customer Support page: https://www.force10networks.com/csportal20/Main/SupportMain.aspx.
2. Log in.
3. Click the BugTrack link, located in the Quick Links menu directly below the login bar.

   This takes you to the BugTrack search page: https://www.force10networks.com/csportal20/BugTrack/SearchIssues.aspx.
4. Enter for a specific PR or select an Dell Networking OS version, platform, Severity, or category to get a list of PRs.
5. Click the Search button.
6. Click the PR number to view specific PR details.

The PR (or PRs) appears on the page below the tool.

The following caveats are open in Dell EMC Networking OS version 9.14(1.9P4):

PR#169841

Severity:	Sev 2
Synopsis:	In certain scenarios, an MSDP learnt PIM TIB entry stays in `registering` state indefinitely.
Release Notes:	In certain scenarios, an MSDP learnt PIM TIB entry stays in `registering` state indefinitely.

Workaround:	Set the affected node as a non-designated router in the RPF neighbor interface.

Support Resources

The following support resources are available for the S4810 system.

Documentation Resources

This document contains operational information specific to the S4810 system.

For information about using the S4810, refer to the following documents at http://www.dell.com/support:

- *Installing the S4810 System*
- *Quick Start Guide*
- *Dell Networking Command Line Reference Guide for the S4810 System*
- *Dell Networking Configuration Guide for the S4810 System*

For more information about hardware features and capabilities, refer to the Dell Networking website at https://www.dell.com/networking.

For more information about the open network installation environment (ONIE)-compatible third-party operating system, refer to http://onie.org.

Issues

Issues are unexpected or incorrect behavior and are listed in order of Problem Report (PR) number within the appropriate sections.

NOTE: You can subscribe to issue update reports or use the BugTrack search tool to read current information about open and closed issues. To subscribe or use BugTrack, visit Dell Support at: https://www.force10networks.com/CSPortal20/BugTrack/SearchIssues.aspx.

Finding Documentation

This document contains operational information specific to the S4810 system.

- For information about using the S4810, refer to the documents at http://www.dell.com/support.
- For more information about hardware features and capabilities, refer to the Dell Networking website at https://www.dell.com/networking.
- For more information about the open network installation environment (ONIE)-compatible third-party operating system, refer to http://onie.org.

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

Go to www.dell.com/support.

Notes, cautions, and warnings

ⓘ **NOTE: A NOTE indicates important information that helps you make better use of your product.**

△ **CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

⚠ **WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**