

Dell PowerEdge M I/O Aggregator 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 on the Dell PowerEdge M I/O Aggregator.

Current Version: 9.14(1.9P4)

Release Date: 2020-07-30

Previous Version: 9.14(1.8)

Topics:

- [Document Revision History](#)
- [Prerequisites](#)
- [Supported Hardware](#)
- [New Dell Networking OS Version 9.14\(1.9P4\) Features](#)
- [Important Points to Remember](#)
- [Restrictions and Known Issues with Other Devices](#)
- [Changes to Default Behavior and CLI Syntax](#)
- [Dell PowerEdge M I/O Aggregator Procedures: Overview](#)
- [Upgrading the Dell Networking OS Image, Boot Flash and Boot Selector Images](#)
- [Upgrading the CPLD](#)
- [VLT Upgrade Procedure](#)
- [Documentation Corrections](#)
- [Deferred Issues](#)
- [Fixed Issues](#)
- [Known Issues](#)
- [Support Resources](#)

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

i 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>. 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.

Prerequisites

The Dell Chassis Management Controller (CMC) version 4.11 or later is required in a Dell PowerEdge M1000e Enclosure to use an M I/O Aggregator module running Dell Networking OS version 9.3(0.0) or later.

You can use the CMC out-of-band management interface to access and manage an M I/O Aggregator using the Dell Networking OS command-line interface. For more information, refer to the Dell Chassis Management Controller Firmware User's Guide on the Dell Support website at <http://support.dell.com/support/edocs/systems/pem/en/index.htm>.

Supported Hardware

The following hardware is supported with this platform:

Hardware
M I/O Aggregator: base module
4-Port 10-Gigabit Ethernet SFP+ module
2-Port 40-Gigabit Ethernet QSFP+ module
4-Port 10GBASE-T module
4-port 2/4/8G FC Flex IO Module

New Dell Networking OS Version 9.14(1.9P4) Features

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

None.

Important Points to Remember

When an Aggregator is installed in an M1000e chassis:

- After you insert any FlexIO module into an empty slot, you must reload the Aggregator for the module to be operational; for example:

```
Jul 24 23:55:55: %I/O-Aggregator:0 %LCMGR-5-OPTIONAL_MODULE_TYPE_MISMATCH: The IOM was
booted with no Optional module in optional slot 1 in stack-unit0, the inserted module
online is QSFP+. Please reload the IOM with the inserted Optional module.
```

- If you remove an installed module and insert a different module type, an error message is displayed to remind you that the slot has been configured for a different type of FlexIO module; for example:

```
Jul 24 23:55:55: %I/O-Aggregator:0 %LCMGR-5-OPTIONAL_MODULE_TYPE_MISMATCH: The IOM was
booted with no Optional module in optional slot 1 in stack-unit 0, the inserted module
online is QSFP+. Please reload the IOM with the inserted Optional module.
```

You must reload the switch to make the FlexIO module operational.

- You can hot swap FlexIO modules of the same type without having to reboot the Aggregator.
- In Dell Networking OS version 9.4(0.0) and later releases, only ESC key can be used to break into the BLI/X-loader of the I/O Aggregator during boot/reload procedure. To use the feature, the user has to upgrade the boot selector as mentioned in the Upgrading the Dell Networking OS Image, Boot Flash and Boot Selector Images.

Restrictions and Known Issues with Other Devices

- While deploying the system in the normal-reload mode in BMP configuration, use the `ip ssh server enable` command at the beginning of the startup configuration if the `write memory` command is used at the end of the configuration.
- An Aggregator supports only one 4-Port 10GBASE-T Module at a time.
- Connections between an Aggregator and the following devices are not supported:
 - Cisco fabric extenders (FEXes): Storage deployments are not supported; LAN deployments are supported.
- Connections between an Aggregator and the following devices are not supported:

- Cisco fabric extenders (FEXes): Storage deployments are not supported; LAN deployments are supported.
- When an Aggregator interoperates with a Brocade B8000 switch, rebooting the Aggregator results in the B8000 switch generating more PFC frames, which may result in the failure to establish the iSCSI sessions.
- In connections with a server using a Q-LOGIC CNA for converged traffic, a FIP snooping session may flap when non-standard LAN traffic is transmitted with SAN traffic.
- In connections with a server using an Intel X520 CNA, the server may fail to boot from the SAN network if a Brocade CNA is also installed in the server.
- 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 Aggregator:
 1. On a server connected to the Aggregator, 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:

```
DellEMC# interface tenGigabitEthernet 0/1
DellEMC(conf-if-te-0/1)# protocol lldp
DellEMC(conf-lldp)# dcbx version cee
DellEMC(conf-lldp)# exit
DellEMC(conf-if-te-0/1)# no shutdown
DellEMC(conf-if-te-0/1)# exit
DellEMC#
```

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
- To ensure interoperability, the recommended LLDP and LACP timeout values that should be configured in devices to which the Aggregator connects (such as ToR switch and servers) are:
 - LLDP timeout: 30 seconds
 - LACP long timeout
- When 68-byte frames are sent at line rate to a server, the server-facing LACP connection may flap. This behavior is due to the server's inability to send LACP control packets when handling incoming line-rate traffic.

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.

Dell PowerEdge M I/O Aggregator Procedures: Overview

To upgrade to the latest Dell Networking OS on a Dell PowerEdge M I/O Aggregator, complete these steps:

- Upgrading the Dell Networking OS Image, Boot Flash and Boot Selector Images
- Upgrading the CPLD

Upgrading the Dell Networking OS Image, Boot Flash and Boot Selector Images

This section describes the procedure to upgrade Boot Flash and Boot Sector Images in Dell PowerEdge M I/O Aggregator.

The Aggregator is pre-loaded with default Dell Networking OS. Each Aggregator must be upgraded individually to a new Dell Networking OS release.

NOTE: Upgrading to Dell Networking OS version 9.14(1.9P4) from a version prior to Dell Networking OS version 8.3.17.3 via TFTP is a two step process.

1. The Dell PowerEdge M I/O Aggregator with Dell Networking OS version prior to 8.3.17.3 must be upgraded to Dell Networking OS 8.3.17.3 to support copy of files greater than 32MB via TFTP.
2. The switch can then be upgraded to Dell Networking OS version 9.14(1.9P4).

NOTE:

- The Dell PowerEdge M I/O Aggregator can be upgraded to Dell Networking OS version 9.14(1.9P4) via TFTP from versions 8.3.17.3 and later without any upgrades to intermediate releases.
- The Dell PowerEdge M I/O Aggregator can be upgraded to Dell Networking OS version 9.14(1.9P4) via FTP and other locations from any previous Dell Networking OS version without any upgrades to intermediate releases.

To upgrade the Dell Networking OS, Boot Flash and Boot Selector Images, follow the below steps:

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: | usbflash:] [A:| B:]
```

EXEC Privilege

```
DellEMC# upgrade system ftp: A:
Address or name of remote host []: 10.16.127.35
Source file name []: FTOS-XL-9.14.1.9P4.bin
User name to login remote host: ftpuser
Password to login remote host:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Erasing IOM Primary Image, please wait
.....
.....!
44875621 bytes successfully copied
System image upgrade completed successfully.
DellEMC#
```

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

```
upgrade system stack-unit [0-5 | 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 [0-5] or on all units by using all in the command.

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

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

```
show boot system stack-unit [0-5 | 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 [0-5]** in the command or for all the stack units by specifying all in the command.

The Dell Networking OS versions present in A: and B: can be viewed for individual units by specifying the stack unit id [0-5] in the command or for all the stack units by specifying all in the command.

```
DellEMC# 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.
DellEMC#
```

5. Upgrade the M I/O Aggregator Boot Flash and Boot Selector image.

```
upgrade boot [all | bootflash-image | bootselector-image] stack-unit [0-5 | all] [booted |
flash: | ftp: | scp: | tftp: | usbflash:] [A: | B:]
```

EXEC Privilege

Dell Networking OS version 9.14(1.9P4) requires M I/O Aggregator Boot Flash image version 4.0.1.3 and Boot Selector image version 4.0.0.2. If any higher versions of Boot Flash or Boot Selector versions are present in the unit, do not upgrade the Boot Flash and Boot Selector images respectively. The Boot Flash and Boot Selector images can be upgraded at the same time by specifying all in the command. These can be upgraded separately by selecting bootflash-image or bootselector-image respectively. The Boot Flash and Boot Selector images can be upgraded for individual stack units by specifying the particular stack unit ID from the range [0-5] in the command. These can be upgraded to all the stack units together by selecting all option instead of the stack unit ID. The Boot Flash and Boot Selector images can be saved in two partitions A: and B: and the user can select the partition to be upgraded by specifying A: or B: in the command.

```
DellEMC# upgrade boot all stack-unit all ftp: A:
Address or name of remote host []: 10.16.127.35
Destination file name []: FTOS-XL-9.14.1.9P4.bin
User name to login remote host: ftpuser
Password to login remote host:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Current Boot information in the system:
=====
Card      BootFlash      Current Version      New Version
-----
Unit0     Boot Flash      4.0.1.1              4.0.1.3
Unit1     Boot Flash      4.0.1.1              4.0.1.3
*****
*Warning - Upgrading boot flash is inherently risky and should only          *
*be attempted when necessary. A failure at this upgrade may cause           *
*a board RMA. Proceed with caution !                                         *
*****
Proceed Boot Flash image for all units [yes/no]: yes
!!!!!!!!!!!!!!!
Erasing IOM Primary Bootflash Image, please wait
.!!.!..!..!..!..!.....
Bootflash image upgrade for all completed successfully.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Current Boot information in the system:
=====
Card      BootSelector    Current Version      New Version
-----
Unit0     Boot Selector   4.0.0.1              4.0.0.2
Unit1     Boot Selector   4.0.0.1              4.0.0.2
*****
*Warning - Upgrading boot selectors is inherently risky and should          *
*only be attempted when necessary. A failure at this upgrade may           *
*cause a board RMA. Proceed with caution !                                   *
*****
Proceed Boot Selector image for all units [yes/no]: yes
!!!
Erasing IOM Boot Selector Image, please wait
.!!.!..!..!..!..!.....
Bootselctor image upgrade for all completed successfully.
DellEMC#
```

6. Change the Primary Boot Parameter of the M I/O Aggregator to the upgraded partition A: or B:

```
boot system stack-unit [0-5 | all] primary [system A: | system B: | tftp://]
```

CONFIGURATION

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

write [memory]

EXEC Privilege

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

8. Reload the unit.

reload

EXEC Privilege

```
DellEMC# 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
```

9. Verify the M I/O Aggregator has been upgraded to the Dell Networking OS version 9.14(1.9P4).

show version

EXEC Privilege

```
DellEMC#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 06:42:55 2020
Build Path: /sites/eqx/work/swbuild01_1/build16/E9-14-1/SW/SRC
Dell Networking OS uptime is 1 day(s), 5 hour(s), 7 minute(s)

System image file is "system://A"

System Type: I/O-Aggregator

Control Processor: MIPS RMI XLP with 2 Gbytes (2147483648 bytes) of memory, core(s) 1.
256M bytes of boot flash memory.

 1 34-port GE/TE/FG (XL)
44 Ten GigabitEthernet/IEEE 802.3 interface(s)
 2 Forty GigabitEthernet/IEEE 802.3 interface(s)
```

10. Verify the M I/O Aggregator has been upgraded to the latest Boot Flash and Boot Selector versions.

show system stack-unit [0-5]

EXEC Privilege

```
DellEMC#show system stack-unit 0

-- Unit 0 --
Unit Type           : Management Unit
Status              : online
Next Boot           : online
Required Type       : I/O-Aggregator - 34-port GE/TE (XL)
Current Type        : I/O-Aggregator - 34-port GE/TE (XL)
Master priority     : 0
Hardware Rev        : X01
Num Ports           : 56
Up Time             : 5 hr, 18 min
Dell Networking OS Version : 9.14(1.9P4)
Jumbo Capable       : yes
POE Capable         : no
FIPS Mode           : disabled
Boot Flash          : A: 4.0.1.3    B: 4.0.1.3 [booted]
Boot Selector       : 4.0.0.2
Memory Size         : 2147483648 bytes
```

```

Temperature      : 51C
Voltage          : ok
Switch Power     : GOOD
Product Name     : DELL I/O Aggregator
Mfg By          : DELL
Mfg Date        :
Serial Number    :
Part Number      : 0NVH81X01
Piece Part ID    : N/A
PPID Revision    : N/A
Service Tag     : N/A
Expr Svc Code    : N/A
Chassis Svce Tag : 29MFHY1
Fabric Id       : B1
Asset tag       :
PSOC FW Rev     : 0xb
ICT Test Date    : 0-0-0
ICT Test Info    : 0x0
Max Power Req    : 31488
Fabric Type      : 0x3
Fabric Maj Ver   : 0x1
Fabric Min Ver   : 0x0
SW Manageability : 0x4
HW Manageability : 0x1
Max Boot Time    : 6 minutes
Link Tuning      : unsupported
Auto Reboot     : enabled
Burned In MAC    : 00:01:e8:01:02:05
No Of MACs      : 3

```

Upgrading the CPLD

An Aggregator with Dell Networking OS version 9.14(1.9P4) requires CPLD image 6.

Verify that a CPLD upgrade is required

Use the following command to identify the CPLD version:

```

DelleMC# show revision

-- Stack unit 0 --
IOM SYSTEM CPLD      : 6

-- Stack unit 1 --
IOM SYSTEM CPLD      : 6

-- Stack unit 2 --
IOM SYSTEM CPLD      : 6

```

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

```

DelleMC#show os-version

RELEASE IMAGE INFORMATION :
-----
Platform      Version      Size      ReleaseTime
IOM-Series:XL  9.14(1.9P4)  46959721  Jul 24 2020 09:07:20

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

BOOT IMAGE INFORMATION :
-----
Type      Version      Target      checksum
boot flash 4.0.1.3      Control Processor  passed

```

BOOTSEL IMAGE INFORMATION :

Type	Version	Target	checksum
boot selector	4.0.0.2	Control Processor	passed

CPLD IMAGE INFORMATION :

Card	CPLD Name	Version
Stack-unit 0	IOM SYSTEM CPLD	6

Upgrading the CPLD Image

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

To upgrade the CPLD image on an Aggregator

1. Upgrade the CPLD image.

```
upgrade fpga-image stack-unit [0-5] booted
```

EXEC Privilege

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

Current FPGA information in the system:

Card	FPGA Name	Current Version	New Version
Unit0	IOM SYSTEM CPLD	6	6

```
*****
* 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 fpga image for stack-unit 0 [yes/no]: yes
```

```
FPGA upgrade in progress!!! Please do NOT power off the unit!!!
!!!!!!!!!!!!!!
```

```
Upgrade result :
```

```
=====
```

```
Unit 0 FPGA upgrade successful. power cycle the stack-unit to complete the upgrade.
```

```
DellEMC#
```

2. Power cycle the switch (IO module) using the CMC interface or remove and re-insert the switch (OIR) from the chassis so that the CPLD upgrade takes effect.

NOTE: The powercycle stack-unit 0 command does not load the latest CPLD version.

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

```
show revision
```

EXEC PRIVILEGE

```
DellEMC# show revision
```

```
-- Stack unit 0 --
IOM SYSTEM CPLD      : 6
```

```
DellEMC#
```


VLT Upgrade Procedure

To upgrade the Dell Networking OS in a VLT setup from version 9.2(0.0) to 9.14(0.1) or later, upgrade the Dell Networking OS to version 9.3(0.0) first. If you are running the Dell Networking OS version 9.3(0.0) or later, you can 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).
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.
7. When all VLT ports are active on the Peer 2, repeat steps 2 through 5 for the Peer 1.

Documentation Corrections

None.

Deferred Issues

Caveats 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 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.

Deferred M I/O Aggregator 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. 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 S/W Caveats for the M I/O Agg in Dell Networking OS Version 9.14(1.9P4)

 **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	<p>S1 — Crash: A software crash occurs in the kernel or a running process that requires a restart of AFM, the router, switch, or process.</p> <p>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.</p> <p>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.</p> <p>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.</p>
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	<p>Work around describes a mechanism for circumventing, avoiding, or recovering from the issue. It might not be a permanent solution.</p> <p>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.</p>

Known S/W Caveats for the M I/O Switch in Dell Networking OS Version 9.14(1.9P4)

The latest information related to Open Caveats is available on iSupport through the BugTrack search tool.

 **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 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 M I/O system.

Documentation Resources

This document contains operational information specific to the M I/O system.

For information about using the M I/O, refer to the following documents at <http://www.dell.com/support>:

- *Installing the M I/O System*
- *Quick Start Guide*
- *Dell Networking Command Line Reference Guide for the M I/O System*
- *Dell Networking Configuration Guide for the M I/O 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 M I/O system.

- For information about using the M I/O, 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.dellemc.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.