



# Cisco NX-OS Software Data Management Engine Remote Code Execution Vulnerability



Advisory ID:	cisco-sa-nxos-dme-rce-cbE3nhZS
First Published:	2020 August 26 16:00 GMT
Last Updated:	2020 August 26 21:13 GMT CVE-2020-3415
Version 1.1:	Final
Workarounds:	No workarounds available
Cisco Bug IDs:	CSCvr89315 CSCvs10167
CVSS Score:	Base 8.8

[Download CSAF](#) [Download CVRF](#) [Email](#)

## Summary

A vulnerability in the Data Management Engine (DME) of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code with administrative privileges or cause a denial of service (DoS) condition on an affected device.

The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to a Layer 2-adjacent affected device. A successful exploit could allow the attacker to execute arbitrary code with administrative privileges or cause the Cisco Discovery Protocol process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition.

**Note:** Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability,

### Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the [Security Vulnerability Policy](#). This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

### Subscribe to Cisco Security Notifications

Subscribe

### Related to This Advisory

[Cisco Event Response: August 2020 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication](#)

#### Your Rating:

☐ ☐ ☐ ☐ ☐

#### Average Rating:

☐ ☐ ☐ ☐ ☐

5 star

4 star

an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Exploitation of this vulnerability also requires jumbo frames to be enabled on the interface that receives the crafted Cisco Discovery Protocol packets on the affected device.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-dme-rce-cbE3nhZS>

This advisory is part of the August 2020 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication, which includes seven Cisco Security Advisories that describe seven vulnerabilities. For a complete list of the advisories and links to them, see [Cisco Event Response: August 2020 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication](#).

## Affected Products

### Vulnerable Products

This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco NX-OS Software:

- Nexus 3000 Series Switches ([CSCvr89315](#))
- Nexus 9000 Series Switches in standalone NX-OS mode ([CSCvr89315](#))
- UCS 6400 Series Fabric Interconnects ([CSCvs10167](#))

For a device to be vulnerable, both of the following conditions must be true:

- DME is enabled.
- Cisco Discovery Protocol is enabled on at least one interface that allows jumbo frames.

For information about which Cisco software releases are vulnerable, see the [Fixed Software](#) section of this advisory.

### Determine the Status of the Data Management Engine

DME is disabled by default on Cisco Nexus 3000 Series Switches that have 4 GB of system memory or less. DME is enabled by default and cannot be disabled on

3 star

2 star

1 star

[Leave additional feedback](#)

Cisco Nexus 3000 Series Switches that have higher system memory.

To determine whether DME is enabled on Cisco Nexus 3000 Series Switches, do the following:

- Verify the amount of system memory by using the **show version | include memory** command in the device CLI. If the memory value is higher than 4 GB (4194304 KB), DME is enabled and cannot be disabled.
- If the memory value is equal to 4 GB or lower, use the **show system dme status** command in the device CLI to verify whether DME is enabled or disabled.

DME is enabled by default on Cisco Nexus 9000 Series Switches and on Cisco UCS 6400 Series Fabric Interconnects and cannot be disabled on these devices.

## Determine the Status of Jumbo Frames

By default, each interface of a Cisco Nexus Switch has a Maximum Transmission Unit (MTU) of 1500 bytes, which is the IEEE 802.3 standard for Ethernet frames. Larger frames, called jumbo frames, are not allowed by default. Administrators can enable jumbo frames by setting a larger MTU with a network Quality of Service (QoS) policy or, on switches that support per-port MTU configuration, by configuring the MTU of the interface itself.

To determine whether jumbo frames are enabled on a Cisco Nexus Switch with a network QoS policy, use the **show policy-map system type network-qos** command in the device CLI. If the command returns an MTU value higher than 1500 bytes, jumbo frames are enabled on the device, as shown in the following example:

```
nxos# show policy-map system type network-qos
Type network-qos policy-maps
=====
policy-map type network-qos jumbo
  class type network-qos class-default
    match qos-group 0
    mtu 9216
```

To determine whether jumbo frames are enabled on an interface of a Cisco Nexus Switch, use the **show running-config interface | include mtu** command in the device CLI. If the command returns at least one line of output, jumbo frames are enabled on at least one interface, as shown in the following example:

```
nxos# show running-config interface | include mtu
mtu 9216
```

Cisco UCS 6400 Series Fabric Interconnects have jumbo frames enabled by default on all interfaces, except the management interface. It is not possible to modify the MTU of physical interfaces on these devices.

## Determine the Status of Cisco Discovery Protocol on Cisco Nexus Switches

Cisco Discovery Protocol is enabled by default both globally and on all interfaces on Cisco Nexus Switches.

To determine whether Cisco Discovery Protocol is enabled on a device, use the **show running-config cdp all | include "cdp enable"** command in the device CLI. If the command returns at least the following lines, Cisco Discovery Protocol is enabled globally and on at least one interface:

```
nxos# show running-config cdp all | include "cdp
enable"
cdp enable
cdp enable
```

## Determine the Status of Cisco Discovery Protocol on Cisco UCS Fabric Interconnects

Cisco Discovery Protocol is always enabled on Ethernet uplink ports (network interfaces that connect to upstream switches for network connectivity), Ethernet port channel members, FCoE uplink ports, and management interfaces of Cisco UCS Fabric Interconnects.

To determine whether Cisco Discovery Protocol is also enabled on server ports (interfaces that are presented to the servers in the Cisco UCS Manager domain) and appliance ports (interfaces that connect to directly attached NFS storage) on a device, use the **show configuration | egrep "^ scope|enable cdp"** command in the device CLI. If the command returns the **enable cdp** command under the **org** scope, Cisco Discovery Protocol is enabled on server ports, and if the command returns **enable cdp** under the **eth-storage** scope, Cisco Discovery Protocol is enabled on appliance ports, as shown in the following example:

```
ucs-fi# show configuration | egrep "^ scope|enable
cdp"
.
```

```
.
.
  scope org
    enable cdp
.
.
.
  scope eth-storage
    enable cdp
.
.
.
```

## Products Confirmed Not Vulnerable

Only products listed in the [Vulnerable Products](#) section of this advisory are known to be affected by this vulnerability.

Cisco has confirmed that this vulnerability does not affect the following Cisco products:

- Firepower 1000 Series
- Firepower 2100 Series
- Firepower 4100 Series
- Firepower 9300 Security Appliances
- MDS 9000 Series Multilayer Switches
- Nexus 1000 Virtual Edge for VMware vSphere
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects

## Workarounds

There are no workarounds that address this vulnerability.

However, customers who do not use the Cisco Discovery Protocol feature can disable it either globally to fully eliminate the attack vector or on individual interfaces to reduce the attack surface.

## Disable Cisco Discovery Protocol Globally on Cisco Nexus Switches

To disable Cisco Discovery Protocol globally on Cisco Nexus Switches, use the **no cdp enable** command in global configuration mode, as shown in the following example:

```
nxos# conf t
Enter configuration commands, one per line. End with
CNTL/Z.
nxos(config)# no cdp enable
nxos(config)# end
nxos# copy running-config startup-config
[#####] 100%
Copy complete.
```

## Disable Cisco Discovery Protocol on an Interface on Cisco Nexus Switches

To disable Cisco Discovery Protocol on an interface on Cisco Nexus Switches, use the **no cdp enable** command in interface configuration mode, as shown in the following example:

```
nxos# conf t
Enter configuration commands, one per line. End with
CNTL/Z.
nxos(config)# interface Ethernet1/1
nxos(config-if)# no cdp enable
nxos(config-if)# end
nxos# copy running-config startup-config
[#####] 100%
Copy complete.
```

## Disable Cisco Discovery Protocol on Cisco UCS Fabric Interconnects

Cisco Discovery Protocol cannot be disabled completely on Cisco UCS Fabric Interconnects.

Cisco Discovery Protocol can be disabled on server ports and appliance ports on Cisco UCS Fabric Interconnects, but it cannot be disabled on Ethernet uplink ports,

Ethernet port channel members, FCoE uplink ports, or management interfaces.

To disable Cisco Discovery Protocol on the server ports of a Cisco UCS Fabric Interconnect, use the **disable cdp** command in the default **nw-ctrl-policy** in the **org** scope, as shown in the following example:

```
ucs-fi# scope org
ucs-fi /org # enter nw-ctrl-policy default
ucs-fi /org/nw-ctrl-policy # disable cdp
ucs-fi /org/nw-ctrl-policy* # exit
ucs-fi /org* # exit
ucs-fi* # commit-buffer
ucs-fi#
```

To disable Cisco Discovery Protocol on the appliance ports of a Cisco UCS Fabric Interconnect, use the **disable cdp** command in the default **nw-ctrl-policy** in the **eth-storage** scope, as shown in the following example:

```
ucs-fi* # scope eth-storage
ucs-fi /eth-storage* # enter nw-ctrl-policy default
ucs-fi /eth-storage/nw-ctrl-policy* # disable cdp
ucs-fi /eth-storage/nw-ctrl-policy* # exit
ucs-fi /eth-storage* # exit
ucs-fi* # commit-buffer
ucs-fi#
```

## Fixed Software

Cisco has released free software updates that address the vulnerability described in this advisory. Customers may only install and expect support for software versions and feature sets for which they have purchased a license. By installing, downloading, accessing, or otherwise using such software upgrades, customers agree to follow the terms of the Cisco software license: <https://www.cisco.com/c/en/us/products/end-user-license-agreement.html>

Additionally, customers may only download software for which they have a valid license, procured from Cisco directly, or through a Cisco authorized reseller or partner. In most cases this will be a maintenance upgrade to software that was previously purchased. Free security software updates do not entitle customers to a new software license, additional software feature sets, or major revision upgrades.

When [considering software upgrades](#), customers are advised to regularly consult the advisories for Cisco products, which are available from the [Cisco Security Advisories page](#), to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

## Customers Without Service Contracts

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco TAC: <https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

## Cisco NX-OS Software

To help customers determine their exposure to vulnerabilities in Cisco NX-OS Software, Cisco provides the [Cisco Software Checker](#) to identify any Cisco Security Advisories that impact a specific Cisco NX-OS Software release and the earliest release that fixes the vulnerabilities that are described in each advisory (“First Fixed”). If applicable, the tool also returns the earliest release that fixes all the vulnerabilities described in all the advisories identified (“Combined First Fixed”).

Customers can use the [Cisco Software Checker](#) to search advisories in the following ways:

- Choose the software, platform, and one or more releases
- Upload a .txt file that includes a list of specific releases
- Enter the output of the **show version** command

After initiating a search, customers can customize the search to include all Cisco Security Advisories or one or more specific advisories.

Customers can also use the following form to determine whether a release is affected by any Cisco Security Advisory by choosing the Cisco NX-OS Software and platform and then entering a release—for example, **7.0(3)I7(5)** for Cisco Nexus 3000



Series Switches or **14.0(1h)** for Cisco NX-OS Software in ACI mode:

Cisco NX-OS Software

MDS 9000 Series Multilayer Switches

By default, the [Cisco Software Checker](#) includes results only for vulnerabilities that have a Critical or High Security Impact Rating (SIR). To include results for Medium SIR vulnerabilities, customers can use the Cisco Software Checker and check the **Medium** check box in the drop-down list under **Impact Rating** when customizing a search.

Cisco UCS Software

In the following table(s), the left column lists Cisco software releases. The center column indicates whether a release is affected by the vulnerability described in this advisory and the first release that includes the fix for this vulnerability. The right column indicates whether a release is affected by all the vulnerabilities described in this bundle and which release includes fixes for those vulnerabilities.

UCS 6400 Series Fabric Interconnects

Cisco UCS Software Release	First Fixed Release for This Vulnerability	First Fixed Release for All Vulnerabilities Described in the Bundle of Advisories
4.0	4.0(4h)	4.0(4i)
4.1	Not vulnerable	4.1(1c)

Additional Resources

For help determining the best Cisco NX-OS Software release for a Cisco Nexus Switch, see the following Recommended Releases documents. If a security advisory recommends a later release, Cisco recommends following the advisory guidance.

- [Cisco MDS Series Switches](#)
- [Cisco Nexus 1000V for VMware Switch](#)
- [Cisco Nexus 3000 Series Switches](#)
- [Cisco Nexus 5500 Platform Switches](#)
- [Cisco Nexus 5600 Platform Switches](#)
- [Cisco Nexus 6000 Series Switches](#)
- [Cisco Nexus 7000 Series Switches](#)
- [Cisco Nexus 9000 Series Switches](#)
- [Cisco Nexus 9000 Series ACI-Mode Switches](#)

To determine the best release for Cisco UCS Software, see the Recommended Releases documents in the release notes for the device.

## Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

## Source

This vulnerability was found by Karthick Murugan of Cisco during internal security testing.

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-dme-rce-cbE3nhZS>

## Revision History

Version	Description	Section	Status	Date
1.1	Fixed Software Checker link.	Fixed Software	Final	2020-AUG-26
1.0	Initial public release.	-	Final	2020-AUG-26

### LEGAL DISCLAIMER

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A standalone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy and may lack important information or contain factual errors. The information in this document is intended for end users of Cisco products.

