Cisco Security Advisory

Cisco FXOS and NX-OS Software Cisco Discovery Protocol Arbitrary Code Execution and Denial of Service Vulnerability

High

Advisory ID: cisco-sa-20200226-fxos-nxos-cdp

First Published: 2020 February 26 16:00 GMT

Last Updated: 2020 March 6 16:42 GMT

CVE-2020-3172

Version 1.1: Final

Workarounds: No workarounds available

Cisco Bug IDs: CSCux07556

CSCux58226

CSCvr31410

More...

CVSS Score:
Base 8.8

Download CSAF Download CVRF Email

Summary

A vulnerability in the Cisco Discovery Protocol feature of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code as *root* or cause a denial of service (DoS) condition on an affected device.

The vulnerability exists because of insufficiently validated Cisco Discovery Protocol packet headers. 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 cause a buffer overflow that could allow the attacker to execute arbitrary code as *root* or cause a DoS condition on the affected device.

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: February 2020 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication

Your Rating:

Average Rating:

5 star

0

Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).

Note: This vulnerability is different from the following Cisco FXOS and NX-OS Software Cisco Discovery Protocol vulnerabilities that Cisco announced on Feb. 5, 2020: Cisco FXOS, IOS XR, and NX-OS Software Cisco Discovery Protocol Denial of Service Vulnerability and Cisco NX-OS Software Cisco Discovery Protocol Remote Code Execution Vulnerability.

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-20200226-fxos-nxos-cdp

This advisory is part of the February 2020 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication, which includes six Cisco Security Advisories that describe six vulnerabilities. For a complete list of the advisories and links to them, see Cisco Event Response: February 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 FXOS Software or Cisco NX-OS Software and if they are configured to use Cisco Discovery Protocol:

- Firepower 4100 Series (**CSCvr37151**)
- Firepower 9300 Security Appliances (**CSCvr37151**)
- MDS 9000 Series Multilayer Switches (**CSCux07556**)
- Nexus 1000 Virtual Edge for VMware vSphere (**CSCvr37146**)
- Nexus 1000V Switch for Microsoft Hyper-V (**CSCvr37146**)
- Nexus 1000V Switch for VMware vSphere (**CSCvr37146**)
- Nexus 3000 Series Switches (**CSCux58226**)
- Nexus 5500 Platform Switches (**CSCvr37148**)
- Nexus 5600 Platform Switches (**CSCvr37148**)
- Nexus 6000 Series Switches (**CSCvr37148**)
- Nexus 7000 Series Switches (**CSCux07556**)

Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode (**CSCvr31410**)
- Nexus 9000 Series Switches in standalone NX-OS mode (**CSCux58226**)
- UCS 6200 Series Fabric Interconnects (**CSCvr37150**)
- UCS 6300 Series Fabric Interconnects (**CSCvr37150**)

Note: Cisco Discovery Protocol is enabled by default both globally and on all interfaces in Cisco FXOS and NX-OS Software.

For information about which Cisco software releases are vulnerable, see the Fixed Software section of this advisory.

Determine the Status of Cisco Discovery Protocol for Cisco FXOS Software

Cisco Discovery Protocol is always enabled on the management (mgmt0) port. In Cisco FXOS Software releases earlier than Release 2.1, Cisco Discovery Protocol is always enabled on all front-panel ports as well.

Determine the Status of Cisco Discovery Protocol on Cisco Nexus Switches That Are Running Cisco NX-OS Software

Administrators can determine whether Cisco Discovery Protocol is enabled on a device by using 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 ports.

Administrators can 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 by using 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 products:

- Firepower 1000 Series
- Firepower 2100 Series
- UCS 6400 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 close the attack vector or on individual interfaces to reduce the attack surface.

Disable Cisco Discovery Protocol in Cisco FXOS Software

Cisco Discovery Protocol is always enabled and cannot be disabled in Cisco FXOS Software. In Cisco FXOS Software releases 2.1 and later, Cisco Discovery Protocol is enabled on the management (mgmt0) port only.

Disable Cisco Discovery Protocol Globally on Cisco Nexus Switches That Are Running Cisco NX-OS Software

To disable Cisco Discovery Protocol globally on Cisco Nexus Switches that are running Cisco NX-OS Software, administrators can 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 That Are Running Cisco NX-OS Software

To disable Cisco Discovery Protocol on an interface on Cisco Nexus Switches that are running Cisco NX-OS Software, administrators can 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 CS Fabric Interconnects, but it cannot be disabled on Ethernet uplink ports,

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

To disable Cisco Discovery Protocol on the server ports of a Cisco UCS Fabric Interconnect, administrators can 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, administrators can 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 and Alerts 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 FXOS 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.

Firepower 4100 Series and Firepower 9300 Security Appliances: CSCvr37151

Cisco FXOS Software Release	First Fixed Release for This Vulnerability	First Fixed Release for all Vulnerabilities Described in the Bundle of Advisories
Earlier than 2.2	Migrate to a fixed release.	Migrate to a fixed release.
2.2	Migrate to a fixed release.	Migrate to a fixed release.
2.3	2.3.1.179	2.3.1.179
2.4	Migrate to a fixed release.	Migrate to a fixed release.
2.6	2.6.1.187	2.6.1.187
2.7	2.7.1.106	2.7.1.106

Note: In Cisco FXOS Software releases 2.1 and later, this vulnerability is exploitable only via the management (mgmt0) port. In these releases Cisco Discovery Protocol is never actually enabled on front-panel ports, even if it is configured.

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

Enter Version	Check

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 6200 and 6300 Series Fabric Interconnects: CSCvr37150

Cisco UCS Software Release	First Fixed Release for This Vulnerability	First Fixed Release for all Vulnerabilities Described in the Bundle of Advisories
Earlier than 3.2	Migrate to a fixed release.	Migrate to a fixed release.
3.2	3.2(3n)	3.2(3n)
4.0	4.0(4g)	4.0(4g)
4.1	Not vulnerable.	Not vulnerable.

Additional Resources

For help determining the best Cisco NX-OS Software release for a Cisco Nexus Switch, administrators can refer to 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, 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 during the resolution of a Cisco TAC support case.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-fxos-nxos-cdp

Revision History

Version	Description	Section	Status	Date
1.1	Added FXOS release.	Fixed Software	Final	2020-March-06
1.0	Initial public release.	-	Final	2020-FEB-26