Cisco Security Advisory

Cisco FXOS and NX-OS Software Cisco Fabric Services Denial of Service Vulnerability

High

Advisory ID:	cisco-sa-fxos-nxos-cfs-dos-dAmnymbd	
First Published:	2020 August 26 16:00 GMT	
Last Updated:	2020 August 26 21:23 GMT	CVE-2020-3517
Version 1.1:	Final	
Workarounds:	No workarounds available	
Cisco Bug IDs:	CSCvt39630 CSCvt46835 CSCvt46837 More...	

CVSS Score:
Base 8.6

Download CSAF Download CVRF Email

Summary

A vulnerability in the Cisco Fabric Services component of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated attacker to cause process crashes, which could result in a denial of service (DoS) condition on an affected device. The attack vector is configuration dependent and could be remote or adjacent. For more information about the attack vector, see the Details section of this advisory.

The vulnerability is due to insufficient error handling when the affected software parses Cisco Fabric Services messages. An attacker could exploit this vulnerability by sending malicious Cisco Fabric Services messages to an affected device. A successful exploit could allow the attacker to cause a reload of an affected device, which could result in a DoS condition.

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

0

4 star

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-fxos-nxos-cfs-dos-dAmnymbd

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 FXOS or NX-OS Software and have Cisco Fabric Services enabled:

- Firepower 4100 Series (CSCvt46839)
- Firepower 9300 Security Appliances (CSCvt46839)
- MDS 9000 Series Multilayer Switches (CSCvt46835)
- Nexus 3000 Series Switches (CSCvt39630)
- Nexus 5500 Platform Switches (CSCvt46837)
- Nexus 5600 Platform Switches (CSCvt46837)
- Nexus 6000 Series Switches (CSCvt46837)
- Nexus 7000 Series Switches (CSCvt46835)
- Nexus 9000 Series Switches in standalone NX-OS mode (CSCvt39630)
- UCS 6200 Series Fabric Interconnects (CSCvt46838)
- UCS 6300 Series Fabric Interconnects (CSCvt46838)
- UCS 6400 Series Fabric Interconnects (CSCvt46877)

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

Determine Whether a Device Has Cisco Fabric Services Enabled

To determine whether a device that is running Cisco FXOS or NX-OS Software has Cisco Fabric Services enabled, use the **show cfs status | include Distribution**

0

3 star

0

2 star

0

1 star

1

Leave additional feedback

command. If the command returns a global **Distribution** state of **Enabled**, the device is vulnerable. If the global **Distribution** state is **Disabled** or this command is not available, the device is not affected by this vulnerability. The following example shows the output of the **show cfs status | include Distribution** command from a device that is vulnerable:

```
nexus# show cfs status | include Distribution
Distribution : Enabled
Distribution over IP : Enabled
Distribution over Ethernet : Disabled
nexus#
```

Note: On Cisco UCS Fabric Interconnects, first execute the **connect nxos** command to enter the NX-OS CLI, then use the **show cfs status | include Distribution** command.

For more information about Cisco Fabric Services and its distribution status, see the Details section of this advisory.

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
- Nexus 1000 Virtual Edge for VMware vSphere
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode

Details

Cisco Fabric Services provides a common infrastructure for distributing and synchronizing configuration data between Cisco devices that are on the same network and with virtual port channels (vPCs) or in Virtual Extensible LAN (VXLAN) deployments. This includes configuration data for applications and features that are compatible with and enabled to use Cisco Fabric Services-for example, Distributed Device Alias Services, Network Time Protocol (NTP), and user and administrator roles.

The vulnerability that is described in this advisory is due to insufficient error handling when the affected software parses Cisco Fabric Services messages. Exploitation of this vulnerability does not require any applications to be enabled to use Cisco Fabric Services. Instead, exploitation depends on which Cisco Fabric Services distribution types are configured for a device. In addition, the attack vectors vary based on which distribution types are configured. If a device is enabled to use more than one distribution type, the applicable attack vectors for all those distribution types exist for the device.

Cisco Fabric Services over Fibre Channel

Distribution	Distributes data over a Fibre Channel, such as a virtual storage area network (VSAN)
Enablement	*Enabled by default* on Cisco MDS 9000 Series Multilayer Switches *Enabled* on Nexus devices if Fibre Channel or Fibre Channel over Ethernet (FCoE) configuration is present
Attack Vector	Attack could occur over Fibre Channel, Fibre Channel over Ethernet (FCoE), or Fibre Channel over IP (FCIP) Attack could succeed in the *data plane*, not the management plane, of any Fibre Channel port If no Fibre Channel and no FCoE ports are configured for a device, this distribution type cannot be used to exploit the vulnerability
CVSS Attack Vector	Adjacent

Cisco Fabric Services over Ethernet

Distribution	Distributes data over an Ethernet network
Enablement	*Disabled by default*
Attack Vector	Attack is possible *from only a vPC peer* or an attacker who has access to a *vPC peer link* No other peer, neighbor, or network node can be used to exploit the vulnerability
CVSS Attack Vector	Adjacent

Cisco Fabric Services over IP

Distribution	Distributes data over an IPv4 or IPv6 network
Enablement	*Disabled by default*
Attack Vector	Attack is possible from any node that has IP network connectivity to the *management interface* of a device Attack *cannot* succeed from the *data plane*
CVSS Attack Vector	Network

Determine the Distribution Status of Cisco Fabric Services

To display configuration information and check the distribution status of Cisco Fabric Services for a device, use the **show cfs status | include Distribution** command in the device CLI, as shown in the following example:

```
switch# show cfs status | include Distribution
Distribution : Enabled
Distribution over IP : Disabled
Distribution over Ethernet : Disabled
```

In the preceding example, the **Enabled** value in the **Distribution** field of the command output indicates that Cisco Fabric Services is enabled for the device and that the device is configured to use the default Cisco Fabric Services distribution type, which is Cisco Fabric Services over Fibre Channel. The **Disabled** value in the **Distribution over IP** field and the **Distribution over Ethernet** field indicates that the device is not additionally configured to use the Cisco Fabric Services over IP or Cisco Fabric Services over Ethernet distribution types.

Workarounds

There are no workarounds that address this vulnerability.

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 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[1]

Cisco FXOS Software Release	First Fixed Release for This Vulnerability	First Fixed Release for all Vulnerabilities Described in the Bundle of Advisories
1.1	1.1.4.179	1.1.4.179
2.0	2.0.1.153	2.0.1.153
2.1	2.1.1.86	2.1.1.86
2.2	2.2.1.70	2.2.1.70
2.3	Not vulnerable	Not vulnerable
2.4	Not vulnerable	Not vulnerable
2.6	Not vulnerable	Not vulnerable
2.7	Not vulnerable	Not vulnerable
2.8	Not vulnerable	Not vulnerable

1. This vulnerability does not affect releases of Cisco FXOS Software that have the fix for the Cisco FXOS and NX-OS Software Cisco Fabric Services Arbitrary Code Execution Vulnerability, which essentially removed support for Cisco Fabric Services from Cisco FXOS Software.

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 Nexus 3000 and 9000 Series Switches Software Maintenance Upgrade

For Cisco Nexus 3000 and 9000 Series Switches, the following software maintenance upgrade (SMU) is available for Cisco NX-OS Software Release 7.0(3)I7(8): *nxos.CSCvt39630-n9k_ALL-1.0.0-7.0.3.I7.8.lib32_n9000.rpm*.

To download the SMU from the Software Center on Cisco.com, do the following:

1. Click **Browse All**.
2. Choose **IOS and NX-OS Software > NX-OS > NX-OS Software > Switches > Data Center Switches**.
3. Choose the appropriate product and model.
4. Choose **NX-OS Software Maintenance Upgrades (SMU)**.
5. Choose Release 7.0(3)I7(8) from the left pane of the appropriate product page.

Note: The SMU filename is *nxos.CSCvt39630-n9k_ALL-1.0.0-7.0.3.I7.8.lib32_n9000.rpm.*

SMU Installation Instructions

To install the SMU, copy the SMU to the *Bootflash:* file system for the switch and execute the following commands, which activate the fix right away (this is a hot patch):

1. **install add bootflash:nxos.CSCvt39630-n9k_ALL-1.0.0-7.0.3.I7.8.lib32_n9000.rpm activate**
2. **install commit**

The following example shows the commands for installing the SMU for Cisco NX-OS Software Release 7.0(3)I7(8):

```
nx-os# install add bootflash:nxos.CSCvt39630-
n9k_ALL-1.0.0-7.0.3.I7.8.lib32_n9000.rpm
activate nx-os# install commit
```

Note: These instructions apply to only this particular type of SMU.

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, 6300, and 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
Earlier than 3.2	Migrate to a fixed release.	Migrate to a fixed release.
3.2	3.2(3o)	3.2(3o)

4.0	4.0(4i)	4.0(4i)
4.1	4.1(1c)	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 during internal security testing.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-nxos-cfs-dos-dAmnymbd

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.