SK

Cisco FXOS and NX-OS Software Unidirectional Link Detection Denial of

Updated: February 24, 2021 **Document ID:** 1614188442851250

Bias-Free Langua

Cisco Security Advisory

Cisco FXOS and NX-OS Software Unidirectional Link Detection Denial of Service and Arbitrary Code Execution Vulnerability

Medium

Advisory ID:
cisco-sa-nxos-udld-rce-xetH6w35

First Published:
2021 February 24 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCvv78238 , CSCvv96088 , CSCvv96090 , More...

CVE-2021-1368

CVSS Score:
Base 8.8 **Click Icon to Copy Verbose Score**
CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:X/RL:X/RC:X

Download CSAF Download CVRF Email

Summary

A vulnerability in the Unidirectional Link Detection (UDLD) feature of Cisco FXOS Software and 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.

This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted Cisco UDLD protocol packets to a directly connected, affected device. A successful exploit could allow the attacker to

execute arbitrary code with administrative privileges or cause the Cisco UDLD process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition.

Note: *The UDLD feature is disabled by default,* and the conditions to exploit this vulnerability are strict. The attacker needs full control of a directly connected device. That device must be connected over a port channel that has UDLD enabled. To trigger arbitrary code execution, both the UDLD-enabled port channel and specific system conditions must exist. In the absence of either the UDLD-enabled port channel or the system conditions, attempts to exploit this vulnerability will result in a DoS condition.

It is possible, but highly unlikely, that an attacker could control the necessary conditions for exploitation. The CVSS score reflects this possibility. However, given the complexity of exploitation, Cisco has assigned a Medium Security Impact Rating (SIR) to this 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-nxos-udld-rce-xetH6w35

Affected Products

Vulnerable Products

At the time of publication, this vulnerability affected the following Cisco products if they were running a vulnerable release of Cisco FXOS or NX-OS Software and had the UDLD feature enabled:

- Firepower 4100 Series (CSCvv96092 / CSCvw38984) [1]
- Firepower 9300 Security Appliances (CSCvv96092 / CSCvw38984) [1]
- MDS 9000 Series Multilayer Switches (CSCvv96088 / CSCvw38981)
- Nexus 3000 Series Switches (CSCvv78238 / CSCvw38964)
- Nexus 5500 Platform Switches (CSCvv96090 / CSCvw38982)
- Nexus 5600 Platform Switches (CSCvv96090 / CSCvw38982)
- Nexus 6000 Series Switches (CSCvv96090 / CSCvw38982)
- Nexus 7000 Series Switches (CSCvv96088 / CSCvw38981)
- Nexus 9000 Series Switches in standalone NX-OS mode (CSCvv78238 / CSCvw38964)
- UCS 6200 Series Fabric Interconnects (CSCvw45654)
- UCS 6300 Series Fabric Interconnects (CSCvw38983)

- UCS 6400 Series Fabric Interconnects (CSCvv96107 / CSCvw38995)

1. Firepower 4100/9300 products do *not* officially support UDLD; however, the CLI includes commands to enable it. These products could be vulnerable only if UDLD has been enabled in error. In such cases, administrators are advised to disable UDLD to fully eliminate exposure to this vulnerability.

For information about which Cisco software releases were vulnerable at the time of publication, see the Fixed Software section of this advisory. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

Determine the Status of the UDLD Feature on Affected Devices

Devices that are running a vulnerable software release and have the UDLD feature enabled are affected by this vulnerability. The following subsections provide details about how to determine whether the UDLD feature is enabled.

Cisco FXOS Software and UCS Fabric Interconnects

To determine whether the UDLD feature is enabled on a device, use the **scope org** command followed by the **show udld-link-policy** commands at the device CLI. The command output will display either *Enabled* or *Disabled* under *Admin State* for the default and for any manually configured UDLD link policy. The following example shows the command output on a device that has UDLD disabled:

```
fxos# scope org
fxos# show udld-link-policy

UDLD link policy:
Name       Admin State UDLD mode
---------- ----------- ---------
default       Disabled    Normal
```

Cisco NX-OS Software

To determine whether the UDLD feature is enabled on a device, use the **show running-config | include "feature udld"** command at the device CLI. If the command returns output, the *udld* feature is configured on the device. The following example shows the command output on a device that has UDLD enabled:

```
nxos# show running-config | include "feature udld"
feature udld
```

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

Workarounds

There are no workarounds that address this vulnerability.

Fixed Software

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.

Cisco FXOS Software

At the time of publication, the release information in the following table(s) was accurate. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability described in this advisory and which release included the fix for this vulnerability.

Firepower 4100 Series and Firepower 9300 Security Appliances

Cisco FXOS Software Release	First Fixed Release for This Vulnerability
Earlier than 2.8	Migrate to a fixed release.[1]

Cisco FXOS Software Release	First Fixed Release for This Vulnerability
2.8	2.8.1.143[1]
2.9	2.9.1.135[1]

1. Firepower 4100/9300 products do *not* officially support UDLD; however, the CLI includes commands to enable it. These products could be vulnerable only if UDLD has been enabled in error. In such cases, administrators are advised to disable UDLD to fully eliminate exposure to this vulnerability.

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 ⌄

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 SMUs

For Cisco Nexus 3000 and 9000 Series Switches, SMUs are available for Cisco NX-OS Software. Customers can download the following SMUs from the Software Center on Cisco.com:

- Release 7.0(3)I7(8): nxos.CSCvv78238-n9k_ALL-1.0.0-7.0.3.I7.8.lib32_n9000.rpm
- Release 7.0(3)I7(9): nxos.CSCvv78238-n9k_ALL-1.0.0-7.0.3.I7.9.lib32_n9000.rpm

For details about downloading and installing SMUs in Cisco NX-OS Software for Cisco Nexus 3000 and 9000 Series Switches, see the Performing Software Maintenance Upgrades section of the appropriate Cisco NX-OS system management configuration guide:

- Cisco Nexus 3000 Series Switches
- Cisco Nexus 9000 Series Switches

See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

Cisco Nexus 7000 Series Switches SMUs

For Cisco Nexus 7000 Series Switches, SMUs are available for Cisco NX-OS Software Release 8.2(6). Customers can download the following SMUs from the Software Center on Cisco.com:

- n7000-s2-dk9.8.2.6.CSCvx15395.bin
- n7700-s2-dk9.8.2.6.CSCvx15395.bin

For details about downloading and installing SMUs in Cisco NX-OS Software for Cisco Nexus 7000 Series Switches, see the Performing Software Maintenance Upgrades section of the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.

See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

Cisco UCS Software

At the time of publication, the release information in the following table(s) was accurate. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability described in this advisory and which release included the fix for this vulnerability.

UCS 6200, 6300, and 6400 Series Fabric Interconnects

Cisco UCS Software Release	First Fixed Release for This Vulnerability
Earlier than 4.0	Migrate to a fixed release.
4.0	4.0(4l)
4.1	4.1(2c)

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 the resolution of a Cisco TAC support case.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-udld-rce-xetH6w35

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	–	Final	2021-FEB-24

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.

▶ Cisco Security Vulnerability Policy

▶ Subscribe to Cisco Security Notifications

▶ Related to This Advisory

Quick Links -

About Cisco

Contact Us

Careers

Connect with a partner

Resources and Legal -

Feedback

Help

Terms & Conditions

Privacy Statement

Cookies

Accessibility

Trademarks

Supply Chain Transparency

Sitemap