SK

Content Saved

View All Saved Content Remove from Saved Content

Cisco Security Advisory

Cisco NX-OS Software IPv6 Netstack Denial of Service Vulnerability

High

Advisory ID:
cisco-sa-nxos-ipv6-netstack-edXPGV7K

First Published:
2021 February 24 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCvu11961 , CSCvu77380

CVE-2021-1387

CWE-401

CVSS Score:
Base 8.6 **Click Icon to Copy Verbose Score**
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:X/RL:X/RC:X

Download CSAF Download CVRF Download PDF Email

Summary

A vulnerability in the network stack of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

This vulnerability exists because the software improperly releases resources when it processes certain IPv6 packets that are destined to an affected device. An attacker could exploit this vulnerability by sending multiple crafted IPv6 packets to an affected device. A successful exploit could cause the network stack to run out of available buffers, impairing

operations of control plane and management plane protocols and resulting in a DoS condition. Manual intervention would be required to restore normal operations on the affected device.

For more information about the impact of this vulnerability, see the Details section of this advisory.

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ipv6-netstack-edXPGV7K

This advisory is part of the February 2021 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see Cisco Event Response: February 2021 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 and have an IPv6 address or **ipv6 forward** configured on at least one interface:

- Nexus 3000 Series Switches (CSCvu11961)
- Nexus 5500 Platform Switches (CSCvu11961)
- Nexus 5600 Platform Switches (CSCvu11961)
- Nexus 6000 Series Switches (CSCvu11961)
- Nexus 7000 Series Switches (CSCvu11961)
- Nexus 9000 Series Switches in standalone NX-OS mode (CSCvu11961)
- UCS 6400 Series Fabric Interconnects (CSCvu77380)

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

Determine the Status of IPv6 on Cisco NX-OS Software

To determine whether a device will accept incoming IPv6 packets, use the **show ipv6 interface brief vrf all** command at the device CLI. A device could be affected by this vulnerability if the command returns an IPv6 interface status from at least one interface, as shown in the following example:

```
Switch# show ipv6 interface brief vrf all
IPv6 Interface Status for VRF "default"(1)
```

```
Interface       IPv6 Address/Link-local Address          Interface Status
                                                         prot/link/admin
Eth1/65         2001:db8:1:f101::1                       up/up/up
                fe80::23a:7dff:fe95:d071

IPv6 Interface Status for VRF "management"(2)
Interface       IPv6 Address/Link-local Address          Interface Status
                                                         prot/link/admin
```

Note: By default, no IPv6 addresses are enabled in Cisco NX-OS Software. An interface of a Nexus device can be configured with an IPv6 address through the **ipv6 address [...]** or **ipv6 link-local [...]** CLI configuration commands. Also, the **ipv6 forward** CLI configuration command can be used to allow an interface to accept IPv6 packets even if no IPv6 address is configured.

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 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects

Details

This vulnerability is due to buffers not freeing properly in the Cisco NX-OS Software network stack known as *netstack*. If an affected device runs out of available buffers, it will stop processing incoming packets for multiple management plane protocols and control plane protocols (including routing protocols). This may cause those protocols to stop working properly on the affected device, resulting in operational failures that could impact traffic and cause a

DoS condition. The impact could depend on the specific platform and the software release on the device. A manual reload of the device is required to restore normal operations.

For this vulnerability to be exploited, the IPv6 traffic must be destined to an affected device. Traffic that transits an affected device cannot be used to exploit this vulnerability.

Indicators of Compromise

Exploitation of this vulnerability could cause the affected device to consume all available network stack buffers and generate error messages similar to the following:

```
2021 Jan 25 16:07:39 nexus %NETSTACK-3-MBUF_FAILED:  netstack [27340]  m_copyin() failed in ipv6_data_mai
2021 Jan 25 16:07:44 nexus %NETSTACK-3-IPV6_API_FAILED:  netstack [27340]  m_copyin() failed in ipv6_proces
```

These error messages could have multiple causes. Customers who observe these messages on a device are advised to contact their support organization to determine whether the messages indicate that the device has been compromised by exploitation of this vulnerability.

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 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 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(4k)	4.0(4k)
4.1	4.1(1e)	4.1(1e)

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ipv6-netstack-edXPGV7K

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

©2023 Cisco Systems, Inc.

© 2023 Cisco and/or its affiliates. All rights reserved.