Cisco IOS and IOS XE Software IPv6 First Hop Security Denial of

Updated: September 23, 2015 **Document ID:** 1454773380319725

Bias-Free Langua

Cisco Security Advisory

Cisco IOS and IOS XE Software IPv6 First Hop Security Denial of Service Vulnerabilities

High

Advisory ID:
cisco-sa-20150923-fhs

First Published:
2015 September 23 16:00 GMT

Last Updated:
2016 December 8 15:19 GMT

Version 1.2: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCuo04400 , CSCus19794

CVE-2015-6278

CVE-2015-6279

CVSS Score:
Base 7.8, Temporal 6.4 **Click Icon to Copy Verbose Score**
AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

Download CSAF Download CVRF Download OVAL Email

Summary

Two vulnerabilities in the IPv6 first hop security feature of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload.

Cisco has released software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities. This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150923-fhs

Note: The September 23, 2015, release of the Cisco IOS and IOS XE Software Security Advisory bundled publication includes three Cisco Security Advisories. All the advisories address vulnerabilities in Cisco IOS

Software and Cisco IOS XE Software. Individual publication links are in *Cisco Event Response: September 2015 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication* at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep15.html

Affected Products

These vulnerabilities affect products running Cisco IOS or Cisco IOS XE Software. See the "Software Versions and Fixes" section of this security advisory for more information about the affected versions of the software.

Vulnerable Products

Devices running a vulnerable version of Cisco IOS or Cisco IOS XE Software are affected by both vulnerabilities if the IPv6 snooping feature from the first-hop security features is configured.
To determine whether the IPv6 snooping feature is configured, use the **show running config | include ipv6 snooping|interface** command and verify that ipv6 snooping is configured on an interface, or use the **show ipv6 snooping policies** command.

The following examples shows the output of these commands on a router with IPV6 snooping configured on the GigabitEthernet0/0/1 interface:

```
router#show running-config | include ipv6 snooping|interface
...
interface GigabitEthernet0/0/1
ipv6 snooping
...

router#show ipv6 snooping policies
Target               Type  Policy               Feature
Target range
Gi0/0/1              PORT  default              Snooping       vlan
all
```

To determine which Cisco IOS Software release is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. If the device is running Cisco IOS Software, the system banner displays text similar to **Cisco Internetwork Operating System Software** or **Cisco IOS Software**. The image name displays in parentheses, followed by the Cisco IOS Software release number and release name. Some Cisco devices do not support the **show version** command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 15.2(4)T1 with an installed image name of *C2951-UNIVERSALK9-M*:

```
Router> show version
Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version
15.5(2)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
!--- output truncated
```

For information about the naming and numbering conventions for Cisco IOS Software, see White Paper: Cisco IOS and NX-OS Software Reference Guide.

Products Confirmed Not Vulnerable

Cisco IOS XR is not affected by these vulnerabilities.
Cisco NX-OS is not affected by these vulnerabilities.
Cisco Wireless LAN Controller (WLC) is not affected by these vulnerabilities.

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

To provide security and scalability, the IPv6 snooping feature bundles several Layer 2 IPv6 first-hop security features, including IPv6 neighbor discovery (ND) inspection, IPv6 device tracking, IPv6 address glean, and IPv6 binding table recovery. IPv6 ND inspection operates either at Layer 2, or between Layer 2 and Layer 3 to provide IPv6 features with security and scalability.

Cisco IOS and IOS XE Software that is configured to use the IPv6 snooping feature is affected by the following two vulnerabilities:

Cisco IOS and IOS XE Software IPv6 Snooping Denial of Service Vulnerability

A vulnerability in the IPv6 snooping feature from the first-hop security features in Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload.

The vulnerability is due to insufficient validation of IPv6 ND packets that use the Cryptographically Generated Address (CGA) option. An attacker could exploit this vulnerability by sending a malformed packet to an affected device where the IPv6 Snooping feature is enabled.

This vulnerability is documented in Cisco bug ID CSCuo04400 (registered customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2015-6279.

Cisco IOS and IOS XE Software IPv6 Snooping Secure Network Discovery Denial of Service Vulnerability

A vulnerability in the IPv6 snooping feature from the first-hop security features in Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload.

The vulnerability is due to insufficient Control Plane Protection (CPPr) against specific IPv6 ND packets. An attacker could exploit this vulnerability by sending a flood of traffic consisting of specific IPv6 ND packets to an affected device where the IPv6 snooping feature is configured.

This vulnerability is documented in Cisco bug ID CSCus19794 (registered customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2015-6278

Workarounds

There are no workarounds for these vulnerabilities.

Administrators may disable the IPv6 snooping feature on an affected device until the device is upgraded to a nonvulnerable release.

To disable IPv6 snooping use the **no ipv6 snooping** command in the interface configuration mode for each interface where the feature has been configured.

To verify that the feature was disabled, use the **show running-config | include ipv6 snooping** command or the **show ipv6 snooping policies** command.

The following example shows a Cisco IOS device with IPv6 snooping disabled:

```
router#show ipv6 snooping policies
Target               Type  Policy               Feature        Target
range
router#
```

Fixed Software

When considering software upgrades, customers are advised to consult the Cisco Security Advisories, Responses, and Alerts archive at http://www.cisco.com/go/psirt and review subsequent advisories 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 IOS Software

Cisco provides a tool to help customers determine their exposure to vulnerabilities in Cisco IOS Software. The Cisco IOS Software Checker allows customers to perform the following tasks:

- Initiate a search by selecting releases from the drop-down menu or uploading a file from a local system
- Enter **show version** command output for the tool to parse

- Create a customized search by including all previously published Cisco Security Advisories, a specific publication, or all advisories in the most recent bundled publication

The tool identifies any Cisco Security Advisories that impact a queried software release and the earliest release that corrects all vulnerabilities in each Cisco Security Advisory ("First Fixed"). If applicable, the tool also returns the earliest possible release that corrects all vulnerabilities in all displayed advisories ("Combined First Fixed"). Please visit the Cisco IOS Software Checker or enter a Cisco IOS Software release in the following field to determine whether the release is affected by any published Cisco IOS Software advisory.

(Example entry: 15.1(4)M2)

Check

For a mapping of Cisco IOS XE Software releases to Cisco IOS Software releases, refer to Cisco IOS XE 2 Release Notes, Cisco IOS XE 3S Release Notes, and Cisco IOS XE 3SG Release Notes.

Cisco IOS XE Software

Cisco IOS XE Software is affected by the vulnerabilities described in this advisory.

Cisco IOS XE Software Train	First Fixed Release for this Advisory	First Fixed Release for All Advisories in the September 2015 Cisco IOS and IOS XE Software Security Advisory Bundled Publication
2.6	Not vulnerable	Vulnerable; migrate to 3.10.6S or later.
3.1S	Not vulnerable	Vulnerable; migrate to 3.10.6S or later.
3.1SG	Not vulnerable	Not vulnerable
3.2S	Not vulnerable	Vulnerable; migrate to 3.10.6S or later.
3.2SE	Vulnerable; migrate to 3.6.3E or later.	Vulnerable; migrate to 3.6.3E or later.
3.2SG	Not vulnerable	Not vulnerable
3.2SQ	Not vulnerable	Not vulnerable
3.2XO	Not vulnerable	Not vulnerable
3.3S	Not vulnerable	Vulnerable; migrate to 3.10.6S or later.
3.3SE	Vulnerable; migrate to 3.6.3E or later.	Vulnerable; migrate to 3.6.3E or later.
3.3SG	Not vulnerable	Not vulnerable
3.3SQ	Not vulnerable	Not vulnerable
3.3XO	Vulnerable; migrate to 3.6.3E or later.	Vulnerable; migrate to 3.6.3E or later.
3.4S	Not vulnerable	Vulnerable; migrate to 3.10.6S or later.
3.4SG	Vulnerable; migrate to 3.6.3E or later.	Vulnerable; migrate to 3.6.3E or later.
3.4SQ	Not vulnerable	Not vulnerable
3.5E	Vulnerable; migrate to 3.6.3E or later.	Vulnerable; migrate to 3.6.3E or later.
3.5S	Not vulnerable	Vulnerable; migrate to 3.10.6S or later.
3.5SQ	Not vulnerable	Not vulnerable
3.6E	3.6.3E	3.6.3E

3.6S	Not vulnerable	Vulnerable; migrate to 3.10.6S or later.
3.7E	3.7.2E	3.7.2E
3.7S	Not vulnerable	Vulnerable; migrate to 3.10.6S or later.
3.8S	Not vulnerable	Vulnerable; migrate to 3.10.6S or later.
3.9S	Vulnerable; migrate to 3.10.6S or later.	Vulnerable; migrate to 3.10.6S or later.
3.10S	3.10.6S	3.10.6S
3.11S	3.11.4S	Vulnerable; migrate to 3.13.3S or later.
3.12S	Vulnerable; migrate to 3.13.3S or later.	Vulnerable; migrate to 3.13.3S or later.
3.13S	3.13.3S	3.13.3S
3.14S	3.14.2S	Vulnerable; migrate to 3.15.1S or later.
3.15S	Not vulnerable	3.15.1S
3.16S	Not vulnerable	Not vulnerable

Exploitation and Public Announcements

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

These vulnerabilities were found during internal testing.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150923-fhs

Revision History

Version	Description	Section	Status	Date
1.2	Updated OVAL definitions are available.			2016-December-08
1.1	Updated Cisco IOS Checker Software Checker form to query all previously published Cisco IOS Software Security Advisories.			2016-January-14

Show Complete History...

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

Cookies / Do not sell or share my personal data

Accessibility

Trademarks

Supply Chain Transparency

Newsroom

Sitemap