Cisco Security Advisory

Cisco IOS XE Software Internet Key Exchange Version 1 Denial of Service Vulnerability

High

Advisory ID:
cisco-sa-iosxe-ikev1-dos-XHk3HzFC

First Published:
2025 May 7 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwi26594

CVE-2025-20192

CWE-232

CVSS Score:
Base 7.7

Download CSAF

Email

Summary

A vulnerability in the Internet Key Exchange version 1 (IKEv1) implementation of Cisco IOS XE Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The attacker must have valid IKEv1 VPN credentials to exploit this vulnerability.

This vulnerability is due to improper validation of IKEv1 phase 2 parameters before the IPsec security association creation request is handed off to the hardware cryptographic accelerator of an affected device. An attacker could exploit this vulnerability by sending crafted IKEv1 messages to the affected device. A successful exploit could allow the attacker to cause the device to reload.

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-iosxe-ikev1-dos-XHk3HzFC

This advisory is part of the May 2025 release of the Cisco IOS and IOS XE Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see Cisco Event Response: May 2025 Semiannual Cisco IOS and IOS XE 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 IOS XE Software and have IKEv1 VPN enabled:

- 1000 Series Integrated Services Routers (ISRs)
- 4000 Series ISRs
- Catalyst 8200 Series Edge Platforms
- Catalyst 8300 Series Edge Platforms
- Catalyst 8500 Series Edge Platforms
- Catalyst 8500L Series Edge Platforms

The following features are affected by this vulnerability if they are configured to use IKEv1:

- Dynamic Multipoint VPN (DMVPN)
- Remote Access IPsec VPN (RAVPN)
- Site-to-Site VPN (S2S VPN)

Note: Cisco Group Encrypted Transport VPN (GET VPN) and SSL VPN do not use IKEv1 for IPsec session establishment and are not affected by this vulnerability.

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

Determine the Device Configuration

1. Determine Whether IKE (v1 or v2) Is Enabled

To determine whether IKE processing is enabled, use the **show ip socket | include 500** or **show udp | include 500** EXEC command on the device CLI. If UDP port 500 or UDP port 4500 is open on a device, the device is processing IKE packets.

Note: UDP ports 500 or 4500 or both will be open regardless of whether IKEv1 or IKEv2 is enabled, as both use the same port and protocol numbers.

The following example shows the output of the **show udp | include 500** command on a device that is processing IKE packets on UDP ports 500 and 4500 using either IPv4 or IPv6:

```
Router#show udp | include 500
 17       --listen--          192.168.1.10      500   0   0 2001011   0
 17(v6)   --listen--          --any--           500   0   0 2020011   0
 17       --listen--          192.168.1.10     4500   0   0 2001011   0
 17(v6)   --listen--          --any--          4500   0   0 2020011   0
```

If this command returns empty output, the device is not affected by this vulnerability. Otherwise, proceed to step 2.

2. Determine Whether IKEv1 Is Used

To determine whether IKEv1 is being actively used by the device, use the **show crypto map** EXEC command on the device CLI. A crypto map uses IKEv1 if it does not have an **IKEv2 Profile** associated. A crypto map is active if there is at least one interface using that crypto map.

The following example shows the output of the **show crypto map** command on a device that has crypto map *CMAP1* configured to use IKEv1 (because no **IKEv2 Profile** is listed) and enabled on interface *GigabitEthernet1*:

```
Router1#show crypto map
Crypto Map IPv4 "CMAP1" 10 ipsec-isakmp
        Peer = 192.168.1.100
        Access-List SS dynamic: False
        Extended IP access list 120
            access-list 110 permit ip 192.168.11.0 0.0.0.255 192.168.12.0 0.0.0.255
        Current peer: 192.168.1.100
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Dualstack (Y/N): N

        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                AESSET:  { esp-256-aes esp-sha256-hmac  } ,
        }
        Interfaces using crypto map CMAP1:
                GigabitEthernet1


Router1#
```

This device is affected by this vulnerability.

The following example shows the output of the **show crypto map** command on a device that has crypto map *CMAP2* configured to use IKEv2 (because an **IKEv2 Profile** is listed) and enabled on interface *GigabitEthernet2*:

```
Router2#show crypto map
Crypto Map IPv4 "CMAP2" 10 ipsec-isakmp
        Peer = 192.168.1.200
        IKEv2 Profile: profile1
        Access-List SS dynamic: False
        Extended IP access list 120
            access-list 120 permit ip 192.168.21.0 0.0.0.255 192.168.22.0 0.0.0.255
        Current peer: 192.168.1.200
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Dualstack (Y/N): N

        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                AESSET:  { esp-256-aes esp-sha256-hmac  } ,
        }
        Interfaces using crypto map CMAP2:
                GigabitEthernet2



Router2#
```

If this is the only crypto map configured on the device, this device is not affected by this vulnerability.

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:

- IOS Software
- IOS XE Software that is running on devices other than those listed in the Vulnerable Products section
- IOS XR Software
- Meraki products
- NX-OS Software

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 with service contracts that entitle them to regular software updates should obtain security fixes through their usual update channels.

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.

The Cisco Support and Downloads page on Cisco.com provides information about licensing and downloads. This page can also display customer device support coverage for customers who use the My Devices tool.

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 IOS and IOS XE Software

To help customers determine their exposure to vulnerabilities in Cisco IOS and IOS XE Software, Cisco provides the Cisco Software Checker. This tool identifies any Cisco security advisories that impact a specific 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 that are described in all the advisories that the Software Checker identifies ("Combined First Fixed").

To use the tool, go to the Cisco Software Checker page and follow the instructions. Alternatively, use the following form to determine whether a release is affected by any Cisco Security Advisory. To use the form, follow these steps:

1. Choose which advisories the tool will search-only this advisory, only advisories with a Critical or High Security Impact Rating (SIR), or all advisories.
2. Enter a release number-for example, **15.9(3)M2** or **17.3.3.**
3. Click **Check**.

Only this advisory ▾

Enter release number [Check]

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-iosxe-ikev1-dos-XHk3HzFC

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2025-MAY-07

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

Your Rating:

★★★★★

Average Rating:

★★★★★

5 star	0
4 star	0
3 star	0
2 star	0
1 star	0

Leave additional feedback