



# Field Notice: FN72510 - Cisco IOS XE Software: Weak Cryptographic Algorithms Are Not Allowed by Default for IPsec Configuration in Certain Cisco IOS XE Software

[Products Affected](#) | [Problem Description](#) | [Problem Symptom](#) | [Workaround/Solution](#)

**Updated:** January 10, 2024 **Document ID:** FN72510

[Bias-Free Language](#)

## Notice

**THIS FIELD NOTICE IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE FIELD NOTICE OR MATERIALS LINKED FROM THE FIELD NOTICE IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS FIELD NOTICE AT ANY TIME.**

## Products Affected

| Affected Software Product | Affected Release | Affected Release Number                               | Comments |
|---------------------------|------------------|---|----------|
| IOS XE Software           | 17               | 17.11.1, 17.11.1a, 17.12.1, 17.13.1, 17.14.1, 17.15.1 |          |

## Defect Information

| Defect ID  | Headline   |
|------------|--|
| CSCwc72588 | Router should not allow weak cryptographic algorithms to be configured for IPsec |

## Problem Description

In releases earlier than the Cisco IOS XE Software releases that are listed in the table in the Workaround/Solution section of this field notice, weak crypto algorithms, including integrity, encryption, and Diffie-Hellman group algorithms, can be configured for IPsec protocol negotiation as well as data plane traffic protection.

In the Cisco IOS XE Software releases that are listed in the table in the Workaround/Solution section of this field notice, weak crypto algorithms are no longer allowed by default due to their weak cryptographic properties. Cisco strongly recommends the use of stronger cryptographic algorithms in their place. To continue to use such weak algorithms, explicit configuration is required. Otherwise, **IPsec tunnel negotiation will fail and cause service disruption as a result.**

The following table lists the IPsec configuration components and algorithms that are affected by this change:

| IPsec Configuration | Command                         | Keyword Deprecated   |
|---------------------|---------------------------------|--|
| IKEv1 Policy        | crypto isakmp policy priority   | encryption {des   3des}<br>hash md5<br>group {1   2   5}                   |
| IKEv2 Proposal      | crypto ikev2 proposal name      | encryption {des   3des}<br>integrity md5<br>group {1   2   5   24}         |
| IPsec Transform-set | crypto ipsec transform-set name | ah-md5-hmac<br>esp-gmac<br>esp-des<br>esp-3des<br>esp-null<br>esp-md5-hmac |

| IPsec Configuration | Command                   | Keyword Deprecated                           |
|---------------------|---------------------------|--|
| IPsec Profile       | crypto ipsec profile name | set pfs {group1   group2   group5   group24} |

## ▼ Background

In Cisco IOS XE Software releases Benaluru 17.6.1 and later, configuration of the IPsec protocol with a weak crypto algorithm generates a warning as shown in this example:

```
Device(config)#crypto isakmp policy 10
```

```
Device(config-isakmp)#encryption des
```

```
%Warning: weaker encryption algorithm is deprecated
```

However, the command is accepted and the weak algorithm can still be used for protocol negotiation for IPsec.

In the Cisco IOS XE Software releases that are listed in the table in the Workaround/Solution section of this field notice, such weak crypto algorithms will be rejected by default and require explicit configuration to be allowed.

## ▼ Problem Symptom

If the IPsec configuration is not updated to use strong cryptographic algorithms before upgrading to one of the Cisco IOS XE Software releases that is listed in the table in the Workaround/Solution section of this field notice, IPsec tunnel negotiation will fail, resulting in service disruption.

## ▼ Workaround/Solution

### Solution (Recommended)

Update the configuration to use strong cryptographic algorithms for IPsec.

### Workaround (Not Recommended)

Enter the following configuration command for IPsec to continue to function with the weak algorithms after upgrading to one of the Cisco IOS XE Software releases that is listed in the table below:

```
Device(config)#crypto engine compliance shield disable
```

**Note:** This command is only available in Cisco IOS XE Software releases 17.7.1 and later and will only take effect after a reboot. Cisco does **not** recommend this option as these weak cryptographic algorithms are insecure and do not provide adequate protection from modern threats. This command should only be used as a last resort.

| Technology         | Cisco Product  | Affected Cisco IOS XE Software Release |
|--------------------|--|--|
| Enterprise Routing | ASR1000 series<br>ISR4000 series<br>ISR1100 series<br>Catalyst 8000 series   | 17.11.1a and later                     |
| Wireless           | Catalyst 9800 Series Wireless Controller<br>Catalyst CG418-E Cellular Gateway<br>Catalyst CG522-E Cellular Gateway<br>Catalyst 9115AX Access Points (APs)<br>Catalyst 9117AX APs<br>Catalyst 9120AX APs<br>Catalyst 9130AX APs | 17.13.1 and later                      |
| SP Access          | ASR920<br>ASR903<br>NCS520   | 17.12.1 and later                      |

| Technology  | Cisco Product  | Affected Cisco IOS XE Software Release |
|-------------|--|--|
|             | NCS4200  |  |
| Switching   | Catalyst 9200 Series<br>Catalyst 9300 Series<br>Catalyst 9400 Series<br>Catalyst 9500 Series | 17.15.1 and later                      |
| IoT Routing | IR1101<br>IR8140H<br>IR1800 Series<br>IR8340<br>ESR6300                                      | 17.14.1 and later                      |

Revision History

| Version | Description  | Section  | Date        |
|---------|--|--|-------------|
| 1.4     | Updated affected releases.   | Problem Description, Background, Problem Symptom, Workaround/ Solution | 2024-JAN-10 |
| 1.3     | Updated the table in Problem Description to include group 24 under IKEv2 Proposal. | Problem Description  | 2023-NOV-21 |
| 1.2     | Updated the Problem Description and Problem Symptom Sections.                      | —  | 2023-APR-10 |
| 1.1     | Updated the Workaround/Solution Section.   | —  | 2023-MAR-15 |
| 1.0     | Initial Release  | —  | 2023-MAR-07 |

For More Information

For further assistance or for more information about this field notice, contact the Cisco Technical Assistance Center (TAC) using one of the following methods:

- Open a service request on Cisco.com
- By email or telephone

Receive Email Notification About New Field Notices

To receive email updates about Field Notices (reliability and safety issues), Security Advisories (network security issues), and end-of-life announcements for specific Cisco products, set up a profile in My Notifications

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

