Field Notice: FN - 72570 - Weak Cryptographic Algorithms Are Not Allowed by Default for OSPF IPsec Configuration in Cisco IOS XE Release 17.11.1 and Later -

Updated: June 29, 2023 **Document ID:** FN72570

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.

Revision History

Revision	Publish Date	Comments
1.0	22-Jun-23	Initial Release

Products Affected

Affected OS Type	Affected Software Product	Affected Release	Affected Release Number	Comments
NON-IOS	IOSXE	17	17.11.1, 17.11.1a	

Defect Information

Defect ID	Headline
CSCwd28106	Deprecate weak cryptographic encryption algorithms used in an OSPFv3 IPsec configuration

Problem Description

In software releases earlier than Cisco IOS® XE Release 17.11.1, weak cryptographic algorithms DES, 3DES, and MD5 can be configured for Open Shortest Path First (OSPF) using the IPsec protocol.

In Cisco IOS XE Release 17.11.1 and later, weak cryptographic 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. In order to continue to use such weak cryptographic encryption algorithms, explicit configuration is required. Otherwise, OSPF neighborship will fail to establish and cause service disruption as a result.

This table lists the OSPF IPsec configurations and algorithms affected by this change.

Command	Keyword Deprecated

`interface <interface-name>`
`   ospfv3 encryption ipsec spi 0x100 esp <encryption type> <authentication type>`
	`{des	3des	md5}`

`router ospfv3 <process>`
`   area <area-id> encryption ipsec spi <spi value> esp <encryption type> <authentication type>`
	`{des	3des	md5}`

`router ospfv3 <process>`
`address-family ipv6 unicast`
`area <area-id> virtual-link <x.x.x.x> encryption ipsec spi <spi value> esp <encryption types> <authentication type>`
	`{des | 3des | md5}`

Background

In Cisco IOS XE Release 17.11.1 and later, such weak cryptographic encryption algorithms will not be allowed by default and require explicit configuration to be allowed.

```
Device(config-router)#area 1 encryption ipsec spi 0x100 esp ?

  aes-cbc  Use AES-CBC encryption

  null     ESP with no encryption

Device(config-router-af)#area 1 virtual-link 1.1.1.1 encryption ipsec spi 0x100 esp ?

  aes-cbc  Use AES-CBC encryption

  null     ESP with no encryption
```

Problem Symptom

If the OSPFv3 IPsec configuration is not updated to use strong cryptographic algorithms prior to the Cisco IOS XE Release 17.11.1 software upgrade, OSPF neighborship will fail to establish and cause service disruption as a result.

Workaround/Solution

Recommended Solution

Before you upgrade the software to Cisco IOS XE Release 17.11.1 or later, update the OSPFv3 IPsec configuration to use strong cryptographic algorithms, specifically AES-CBC for encryption and SHA1 for authentication.

Workaround

This is a workaround only and not the recommended solution.

Enter this configuration command for OSPFv3 IPsec in order to continue to function with the weak algorithms upon an upgrade to Cisco IOS XE Release 17.11.1.

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

Note: This command is only available in Cisco IOS XE Release 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.

For More Information

If you require further assistance, or if you have any further questions regarding this field notice, please contact the Cisco Systems Technical Assistance Center (TAC) by one of the following methods:

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

Receive Email Notification For New Field Notices

My Notifications—Set up a profile to receive email updates about reliability, safety, network security, and end-of-sale issues for the Cisco products you specify.

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