

# Cisco IOS-LPWA Access Vulnerability



Severity: **High** | ID: [CVE-2020-3426](#)

Published: 2020-09-24 16:00

Version: 1.0 : Final

CVSS v3: 7.5

Workarounds: No workarounds available

Cisco ID: [CSCvr53526](#)

This advisory describes a vulnerability in Cisco Industrial and Connected Grid routers.

## Affected Products

Cisco 800 Series Industrial Routers (e.g., Cisco 880, Cisco 890)

Cisco 1000 Series Connected Grid Routers (e.g., Cisco 1000, Cisco 1010)

Cisco Low Power Wide Area (LPWA) Routers (e.g., Cisco 1000LPWA, Cisco 1010LPWA)

Cisco VLPWA Routers (e.g., Cisco 1000VLPWA, Cisco 1010VLPWA)

Cisco Industrial and Connected Grid Routers (e.g., Cisco 800, Cisco 1000, Cisco 1000LPWA, Cisco 1010, Cisco 1010LPWA)

This vulnerability has been assigned the identifier CVE-2020-3426. It is a critical security issue that could allow an attacker to gain unauthorized access to the affected devices.

The vulnerability is caused by a flaw in the way the device handles certain types of network traffic. An attacker could exploit this flaw to send malicious traffic that would cause the device to crash or become unresponsive, potentially leading to a denial-of-service condition.

We recommend that all users of the affected products immediately update their devices to the latest version of the software to fix this vulnerability.

The affected products are listed below:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-lpwa-access-cXsD7PRA>

This advisory was first published on September 24, 2020. It is intended to provide information about a security vulnerability in Cisco Industrial and Connected Grid routers. Cisco is not responsible for any damage or loss that may result from the use of this information. Cisco recommends that all users of the affected products immediately update their devices to the latest version of the software to fix this vulnerability.

[Response: September 2020 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication](#)

## È©²å¹/₂“È£¹/₂å“?

È,,†å¹/₄±æ€§ã®ã,ã,<È£¹/₂å“?

ã“ã®è,,†å¹/₄±æ€§ã“ã€è,,†å¹/₄±ãª Cisco IOS

ã,½ãf•ãf^ã,|ã,§ã,çãfªãfªãf¹/₄ã,¹ã,’å®Ýè;Œã—ã€VLPWA

ãŒæœ‰oåŠ¹ã«ãªãFã|ã„ã,<æ¬jã®ã,·ã,³è£¹/₂å“ã«å½±éÝ;ã,’åŠã¹/₄ã—ã³/₄

- 807 ç”£æ¥ç”’ ISR
- 809 ç”£æ¥ç”’ ISR
- 829 ç”£æ¥ç”’ ISR
- CGR 1000 ãf<ãf¹/₄ã,¿

È,,†å¹/₄±æ€§ãŒå~åœ”ã™ã,<Cisco

ã,½ãf•ãf^ã,|ã,§ã,çãfªãfªãf¹/₄ã,¹ã«ãªã„ã|ã“ã€ã“ã®ã,çãf‰oãfãã,¤ã,¶ãfªã®ã€ãŒã

## VLPWA

ã,¤ãf³ã,¿ãf¹/₄ãf•ã,§ã,¤ã,¹ãŒæœ‰oåŠ¹ã«ã®ãŒã®ãtã«ã,’å~¤æ-ã®ã™ã,<

## VLPWA

ã,¤ãf³ã,¿ãf¹/₄ãf•ã,§ã,¤ã,¹ãŒæœ‰oåŠ¹ã«ã®ãŒã®ãtã«ã,’å~¤æ-ã®ã™ã,<ã«ã“ã€CLI

ã®§ show control-plane host open-ports EXEC

ã,³ãfžãf³ãf‰oã,’ä½ç””ã—ã³/₄ã®ã™ã€,ãf‡ãfãã,¤ã,¹ã®§ TCP ãfãf¹/₄ãf^ 5888

ãŒè§Œæ”³/₄ã•ã,Œã®|ã„ã,<å’å~ã€VLPWA

ã,¤ãf³ã,¿ãf¹/₄ãf•ã,§ã,¤ã,¹ãŒæœ‰oåŠ¹ã«ãªã,§ã€VLPWA

ãf—ãfãf^ã,³ãf«ãfçãf‡ãf ãf;ãffã,»ãf¹/₄ã,ãŒå‡|ç®ãtã®ã,Œã®³/₄ã®ã™ã€,

æ¬jã®ä³/₄ã“ã€VLPWAã,¤ãf³ã,¿ãf¹/₄ãf•ã,§ã,¤ã,¹ãŒæœ‰oåŠ¹ã«ãªãFã|ã®ã,§ã€ã,ã®ã,¹ã®§ 5888ã«IPãfãf¹/₄ã,ãf§ãf³4(IPv4)ã³/₄ã®Yã“IPãfãf¹/₄ã,ãf§ãf³6(IPv6)ã®ã„ã®ã,Œã®ã<ã,control-plane host open-portsã,³ãfžãf³ãf‰oã®å‡åŠ›ã,’ç¤ºã—ã®|ã„ã®³/₄ã®ã™ã€,

<#root>

Router#

show control-plane host open-ports

Active internet connections (servers and established)				
Prot	Local Address	Foreign Address	Service	State
tcp				

\* : 5888

\* : 0

VLPWA Proc LISTEN

è,,†å¼±æ€§ã,’å♦«ã,”ã♦§ã♦,,ã♦ªã♦,,ã♦”ã♦”ã♦Œç¢ºèª♦ã♦•ã,Œã♦Ýè£½å”♦

ã♦”ã♦®ã,çãf‰oãf♦ã,¤ã,¶ãfªã♦®[æ€§ã♦®ã,ã,è£½å”♦ã,»ã,¬ã,·ãf§ãf³ã♦«è”“è½‰ã♦•ã](#)

ã,·ã,¹ã,³ã♦¬ã€♦ã♦”ã♦®è,,†å¼±æ€§ã♦Œä»¥ä,«ã♦®ã,·ã,¹ã,³è£½å”♦ã♦«ã♦¬å½±éÝ;ã,’ä,žã♦^ã♦

- 800 ã,·ãfªãf½ã,ºã,µf½ãf“ã,¹ç¶å♦^åž<ãf«ãf½ã,;
- 2000 ã,·ãfªãf½ã,º Connected Grid ãf«ãf½ã,;
- IOS XE ã,½ãf•ãf^ã,|ã,§ã,¢
- IOS XR ã,½ãf•ãf^ã,|ã,§ã,¢
- NX-OS ã,½ãf•ãf^ã,|ã,§ã,¢

è©³ç’°

Cisco ISR å♦Šã,^ã♦³ Connected Grid ãf«ãf½ã,¿ã♦§ã€♦VLPWA

ã,¤ãf³ã,¿ãf½ãf•ã,§ã,¤ã,¹ã,’æœ‰oåŠ¹ã♦«ã♦™ã,«ã♦”ã€♦LoRaWAN ç”“ã♦®ã,·ã,¹ã,³  
ãf¬ã,¤ãf¤ãf¬ã,¹

ã,²ãf½ãf^ã,|ã,§ã,¤ã♦®ã,¹ãftãf½ã,¿ã,¹ã,’è”å®šã♦Šã,^ã♦³ãfçãf<ã,¿ã♦§ã♦?ã♦³/4ã♦™ã€,ã♦”ã,Œã♦  
Internet of Thingsï¼^IoTi¼‰æ<¡å¼µãfçã,ãf¥ãf½ãf«ã,·ãfªãf½ã,ºã♦® 1  
ã♦¤ã♦§ã€♦ã♦”ã,Œã♦«ã,^ã,Šã€♦ã,³ãf♦ã,¬ãftãffãf‰oãf‡ãf♦ã,¤ã,¹ã♦§ LPWA  
ã,çã,¬ã,»ã,¹ã♦Œå♦¬è£½ã♦«ã♦”ã,Šã♦³/4ã♦™ã€,

è©²å½“ãf‡ãf♦ã,¤ã,¹ã♦® VLPWA ã,¤ãf³ã,¿ãf½ãf•ã,§ã,¤ã,¹ã♦§ã€♦lpwa modem authentication  
mandatory enable

æ©Ýè£½ã♦Œæœ‰oåŠ¹ã♦«ã♦”ã♦Fã♦|ã♦,,ã,«ã♦”ã♦@è,,†å¼±æ€§ã♦®ã,♦æFå^©ç”“ã♦  
VLPWA ã,¤ãf³ã,¿ãf½ãf•ã,§ã,¤ã,¹ã♦§ã€♦lpwa modem authentication mandatory enable  
æ©Ýè£½ã♦Œæœ‰oåŠ¹ã♦«ã♦”ã♦Fã♦|ã♦,,ã,«ã♦”ã♦,å’å♦^ã€♦ã,♦æFå^©ç”“ã♦«ã,^ã♦Fã♦|ã♦”ã♦

æ¬|ã♦®ä³/4ã♦¬ã€♦lpwa modem authentication mandatory

enableæ©Ýè£½ã♦Œæœ‰oåŠ¹ã♦«ã♦”ã♦Fã♦|ã♦,,ã,«VLPWAã,¤ãf³ã,¿ãf½ãf•ã,§ã,¤ã,¹ã,’æŒ♦ã♦¤ãf

running-config interface virtual lpwa 1| include authentication mandatory

enableã,³ãfžãf³ãf‰oã♦®å‡ºåŠ›ã,’ç¤ºã♦—ã♦|ã♦,,ã♦³/4ã♦™ã€,

<#root>

Router#



# Cisco IOS 12.2(3) IOS XE 1.2af-f3.0 | Cisco Software Checker

Cisco IOS 12.2af-f3.0 IOS XE

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

## Cisco Software Checker

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

First Fixed 1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

## 1.2af-f3.0 | Cisco Software Checker

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

- 1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0
- cisco1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0
- show version | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

Check

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0

1.2af-f3.0 | Cisco Software Checker | Cisco IOS XE 1.2af-f3.0



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。