

# Cisco

## FXOS arbitrary file write (CVE-2023-20234) in Cisco IOS XE



Cisco IOS XE, **CVE-2023-20234**: cisco-sa-fxos-

arbitrary-file-BLk6YupL

[20234](#)

Published: 2023-08-23 16:00

Product: Cisco IOS XE 1.0: Final

CVSS Score: **4.4**

Workarounds: No workarounds available

Cisco Bug ID: [CSCwd35726](#) [CSCwb91812](#)

[CSCwd05772](#) [CSCwd35722](#)

**Summary:** In Cisco IOS XE, an arbitrary file write vulnerability exists in the FXOS component. An attacker can exploit this vulnerability to write files to the device's file system.

### Details

Cisco

FXOS arbitrary file write (CVE-2023-20234) in Cisco IOS XE. The vulnerability exists in the FXOS component, which is used for network management.

The vulnerability is caused by a buffer overflow in the FXOS component. An attacker can exploit this vulnerability to write files to the device's file system.

The vulnerability affects Cisco IOS XE versions 17.9(3) and earlier. Cisco has released a patch for this vulnerability in Cisco IOS XE version 17.9(4).

For more information, see the Cisco Security Advisory <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-arbitrary-file-BLk6YupL>.

**References:** Cisco Security Advisory <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-arbitrary-file-BLk6YupL>

FXOS arbitrary file write (CVE-2023-20234) in Cisco IOS XE

OS arbitrary file write (CVE-2023-20234) in Cisco IOS XE. The vulnerability exists in the OS component, which is used for network management.

[FXOS arbitrary file write \(CVE-2023-20234\) in Cisco IOS XE](#)

[OS arbitrary file write \(CVE-2023-20234\) in Cisco IOS XE](#)

### Conclusion

The vulnerability is a medium severity issue. It affects Cisco IOS XE versions 17.9(3) and earlier. Cisco has released a patch for this vulnerability in Cisco IOS XE version 17.9(4).

For more information, see the Cisco Security Advisory <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-arbitrary-file-BLk6YupL>.

FXOS arbitrary file write (CVE-2023-20234) in Cisco IOS XE. The vulnerability exists in the FXOS component, which is used for network management.

- firepower 1000ã, ·ãfªãf¹⁄₄ã, °(CSCwd35726ã€⚡CSCwd05772)
- firepower 2100ã, ·ãfªãf¹⁄₄ã, °(CSCwd35726ã€⚡CSCwd05772)
- firepower 4100ã, ·ãfªãf¹⁄₄ã, °(CSCwb91812ã€⚡CSCwd35722)
- firepower 9300ã, »ã,ãfªãfªãfªãfªã,£ã,çãf—ãf©ã,ªã,çãf³ã,¹(CSCwb91812ã€⚡CSCwd35722)
- Secure Firewall 3100ã, ·ãfªãf¹⁄₄ã, °(CSCwd35726ã€⚡CSCwd05772)

è,,†ã¹⁄₄±æ€§ã⚡CEã~ãce`ã⚡™ã, < Cisco

ã,½ãf·ãf^ã,|ã,šã,çãfªãfªãf¹⁄₄ã,¹ã⚡«ã⚡ªã⚡,,ã⚡|ã⚡\_ã€⚡ã⚡"ã⚡®ã,çãf%ããf⚡ã,ªã,¶ãfªã⚡®ã€CEã

è,,†ã¹⁄₄±æ€§ã, 'ã⚡«ã, "ã⚡šã⚡,,ã⚡ªã⚡,,ã⚡"ã⚡`ã⚡CEçç°èªã⚡•ã,CEã⚡Yè£¹⁄₂ã"⚡

ã⚡"ã⚡®ã,çãf%ããf⚡ã,ªã,¶ãfªã⚡®è,,†ã¹⁄₄±æ€§ã⚡®ã⚡\_ã, <è£¹⁄₂ã"⚡ã,»ã, \_ã,ãfšãf³ã⚡«è`~è¹⁄₄%ã⚡•ã

ã,ã,¹ã,³ã⚡\_ã€⚡ã⚡"ã⚡®è,,†ã¹⁄₄±æ€§ã⚡CEã»ªã,ã⚡®ã,ã,¹ã,³è£¹⁄₂ã"⚡ã⚡«ã⚡\_ã¹⁄₂±éY;ã,'ã,Žã⚡^ã⚡

- MDS 9000ã, ·ãfªãf¹⁄₄ã, °ãfžãf«ãf⚡ãf-ã,ªãfªã,¹ã,ªãffãf⚡
- VMware vSphereã'ã⚡'Nexus 1000 Virtual Edge
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 3000ã, ·ãfªãf¹⁄₄ã, °ã,¹ã,ªãffãf⚡
- Nexus 5500ãf—ãf©ãfãf^ãf•ã,©ãf¹⁄₄ãfã,¹ã,ªãffãf⚡
- Nexus 5600ãf—ãf©ãfãf^ãf•ã,©ãf¹⁄₄ãfã,¹ã,ªãffãf⚡
- Nexus 6000ã, ·ãfªãf¹⁄₄ã, °ã,¹ã,ªãffãf⚡
- Nexus 7000ã, ·ãfªãf¹⁄₄ã, °ã,¹ã,ªãffãf⚡
- ACIãfçãf¹⁄₄ãf%ã⚡®Nexus 9000ã, ·ãfªãf¹⁄₄ã, °ãf•ã,;ãf-ãfªãffã, \_ã,¹ã,ªãffãf⚡
- ã,¹ã,çãf³ãf%ã⚡,çãfãf³NX-OSãfçãf¹⁄₄ãf%ã⚡®Nexus 9000ã, ·ãfªãf¹⁄₄ã, °ã,¹ã,ªãffãf⚡
- UCS 6200ã, ·ãfªãf¹⁄₄ã, °ãf•ã,;ãf-ãfªãffã, \_ã,ªãf³ã,çãf¹⁄₄ã,³ãf⚡ã, \_ãf^
- UCS 6300ã, ·ãfªãf¹⁄₄ã, °ãf•ã,;ãf-ãfªãffã, \_ã,ªãf³ã,çãf¹⁄₄ã,³ãf⚡ã, \_ãf^
- UCS 6400ã, ·ãfªãf¹⁄₄ã, °ãf•ã,;ãf-ãfªãffã, \_ã,ªãf³ã,çãf¹⁄₄ã,³ãf⚡ã, \_ãf^
- UCS 6500ã, ·ãfªãf¹⁄₄ã, °ãf•ã,;ãf-ãfªãffã, \_ã,ªãf³ã,çãf¹⁄₄ã,³ãf⚡ã, \_ãf^

## ã»žé⚡ç-

ã⚡"ã⚡®è,,†ã¹⁄₄±æ€§ã⚡«ã¹⁄₄ã†|ã⚡™ã, <ã»žé⚡ç-ã⚡\_ã⚡,ã,šã⚡¾ã⚡»ã, "ã€,

## ãç®æ£æ, ^ã⚡çã,½ãf·ãf^ã,|ã,šã,ç

ã,½ãf·ãf^ã,|ã,šã,çã⚡®ã,çãffãf—ã,ãf-ãf¹⁄₄ãf%ã⚡, 'æªœè`Žã⚡™ã, <és>ã⚡«ã⚡\_ã€⚡ã,ã,¹ã,³

ã,»ã,ãfªãfªãfªã,£ã,çãf%ããf⚡ã,ªã,¶ãfªã

ãfšãf¹⁄₄ã,ã⚡šã...ªæ%ã⚡šã⚡⚡ã, <ã,ã,¹ã,³è£¹⁄₂ã"⚡ã⚡®ã,çãf%ããf⚡ã,ªã,¶ãfªã, 'ã®šæœYçš,,ã⚡«ã⚡,ç

ã,½ãfªãfªãf¹⁄₄ã,ãfšãf³ã,€ã¹⁄₄ã, 'çç°èªã⚡—ã⚡|ã⚡\_ã⚡\_ã⚡\_ã⚡\_ã⚡\_ã⚡,,ã€,

Technical Assistance Center  
Cisco FXOS

### Cisco FXOS

Software

Fixed

#### Software

Checker

Fixed

#### Checker

First Fixed

Cisco Software

Checker

1. ASA
2. Firepower 1000, Firepower 3100, ASA
3. Firepower 4100
4. Check

2	Critical, High, Medium
Cisco FXOS	
Enter release number	Check

Cisco Product Security Incident Response Team

Cisco Product Security Incident Response

Team

å†°å...

æœ-è,†å!4±æ€§ã-ã€ã,ã,1ã,³ãt...éf"ãšã®ã,»ã,ãfãfãfãfã,£ãfã,1ãfã«ã,^ã£ã!ç™°è!ã•ã,£ã¾ã-ãÿã€,

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-arbitrary-file-BLk6YupL>

æ”¹è,å±ÿæ´

ãfãf¼ã,ãfšãf³	èª-æž	ã,»ã,ã,ãfšãf³	ã,1ãfãf¼ã,¿ã,1	æ-ÿã»
1.0	å^åžå...-é-ãfãfãf¼ã,1	â€	Final	2023å¹8æœ^23æ-ÿ

å^©ç”è!ç´,,

æœ-ã,çãf%ãfã,ã,ã,¶ã,¶ãfãç,,jãçè"¼ã®ã,,ã®ã"ã-ã|ã"æã¾ã-ã|ãšã,šã€æœ-ã,çãf%ãfã,ã,ã,¶ãfã®æf...å±ãšã,^ã³ãfãf³ã,ã®ã½ç"ã«é-çã™ã,«è²-ã»ã®ã,ã¾ãÿã€ã,ã,1ã,³ã-æœ-ãf%ã,ãfãfãfãfã®ãt...ã®1ã,'ã°ãšãã-ã«ã%æ´ã-ãæœ-ã,çãf%ãfã,ã,ã,¶ãfã®è"~èç°ãt...ã®1ã«é-çã-ã|æf...å±è...ãçjã® URLã,çœçç¥ã-ã€ãççç-ã®è»çè¼%ã,,,æ,,è³ã,'æ-½ã-ãÿã´ã^ã€ã½"ç¾ã£çççã"ã®ãf%ã,ãfãfãfãfã®æf...å±ã-ã€ã,ã,1ã,³è£½ã"ã®ã,"ãfãf%ãfãf¼ã,¶ã,ã¾è±jã

## 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。