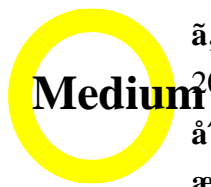


SSH ACL Bypass on Cisco IOS XR



Cisco-SA-20191120-iosxr-ssh-bypass

[CVE-2019-15998](#)

Published: 2019-11-20 16:00

Last Modified: 2019-11-23 02:24

Version: 1.1 : Final

CVSS Score: 5.3

Workarounds: No workarounds available

Cisco ID: [CSCvp91299](#)

SSH Access Control List Bypass on Cisco IOS XR

Summary

This vulnerability affects Cisco IOS XR devices running SSH Access Control List (ACL) configuration.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

The vulnerability is located in the SSH Access Control List (ACL) configuration on Cisco IOS XR devices.

è©²å½“è£½å“

è,†å¼±æ€šã®ã,ã,è£½å“

å†°ç%ç%ç%ã®æ™,ã«ã€ã“ã®è,,†å¼±æ€šã™ Cisco IOS XR å,½åf•åf^å,|å,šå,ç
åfªåfªåf¼å,¹ 6.5.1ã€6.5.2ã€ãšã,^å³ 6.5.3 å«è©²å½“ã—ã¾ã—ãÿã€,
ã“ã®è,,†å¼±æ€šã™ã»-ã®ã©ã®ãfªåfªåf¼å,¹ã«ã,,è©²å½“ã—ã¾ã»ã,“ã€,
æœ€ã,,å®€ã...ãªãç¾ãœã®æf...å±ã«ãªã,,ã|ã-ã“ã®ã,çåf%åfã,ªã,¶åfª
ã®è³ç°ã,,ã-,ãfšãf³ã,ãç...šã—ã|ã,ã•ã,,ã€,

è,†å¼±æ€šã,ª«ã,“ãšã,,ãªã,,ã“ã”ãçç°èªã•ã,ãÿè£½å“

ã“ã®ã,çåf%åfã,ªã,¶åfªã®è,,†å¼±æ€šã™ãœã“ã™ã,è£½å“ã®ã,,ã-,ã,ãfšãf³ã«ãf
Cisco å-ã“ã®è,,†å¼±æ€šã™æ Cisco IOSã,½åf•åf^å,|å,šå,çã« Cisco IOS XE
å,½åfªåf^å,|å,šå,çã«å½±éÿã,ãžã^ãªã,,ã“ã”ã,çç°èªã—ã¾ã—ãÿã€,

åžéç-

ã“ã®è,,†å¼±æ€šã™ã«ã¾å†|ã™ã,åžéç-ã-ã,ã,šã¾ã»ã,“ã€,

ä:®æ£æ,^ãçã,½åf•åf^å,|å,šå,ç

å,½åf•åf^å,|å,šå,çã®ã,çåffåf—ã,°åf-åf¼åf%åã,æœœè”žã™ã,«és>ã«ã-ã€[Cisco Security](#)
[Advisories and Alerts](#)

[åfšåf¼å](#),ãšã...¥æ%åšããã,ã,ã,¹ã,³è£½å“ã®ã,çåf%åfã,ªã,¶åfªã,ã®šæœÿçš,,ã«ãç,
å,½åfªåfªåf¼å,ãfšãf³ã,çç°èªã—ã¾ã|ããããã•ã,,ã€,

ã,,ãšã,ã®ãå’ã^ã,,ã€ã,çåffåf—ã,°åf-åf¼åf%åã™ã,ãf†åfã,ªã,¹ã«ããå†åfªåfçã
ã,æ~žãªç,¹ã«ãªã,,ã|ã-ã€ Cisco Technical Assistance
Center¼^TAC¼%å,,ã—ããã-ã¥ç’,ã—ã|ã,,ã,ãfªf³åf†åfšãf³ã,¹
åf—åfåfã,ªåfåf¼å«ãšã•ãã,å^ã,ãã»ããããã•ã,,ã€,

ä:®æ£æ,^ãçãfªåfªåf¼å,¹

å†°ç%ç%ç%ã®æ™,ã«ã€ãSMU åšã,^ã³ããã,ã«ã¥é™ã® Cisco IOS XR
å,½åfªåf^å,|å,šå,ç åfªåfªåf¼å,¹ 6.5.3
ã-ã“ã®è,,†å¼±æ€šã™ãÿã,ãã®ä:®æ£æãœã«¾ã,ãã|ã,,ã¾ã—ãÿã€,
æœ€ã,,å®€ã...ãªãç¾ãœã®æf...å±ã«ãªã,,ã|ã-ã“ã®ã,çåf%åfã,ªã,¶åfªã

ã⚡@è³ç´° ã,»ã,¯ã,·ãfšãf³ã,'ã⚡,ç...šã⚡—ã⚡|ã,ã⚡·ã⚡,,ã€,

é;šã@çã⚡ Software Center ã⚡<ã,%oæ¬;ã⚡@ä½œæ¥ã,'è;CEã⚡†ã⚡"ã⚡"ã⚡«ã,^ã⚡£ã⚡| SMU ã,'ãf€ã,|ãf³ãfãf¼ãf%oã⚡šã⚡ã⚡ã⚡¾ã⚡™:

1. [ã⚡™ã⚡¹ã⚡|ã⚡,ç...šã⚡^Browse alli¼%o] ã,ã,¯ãf³ãfãfã,¯ã⚡—ã⚡¾ã⚡™ã€,
2. > ã,µf¼ãf"ã,¹ãf—ãfãfã⚡ã,µãf€ãf¼ã,ã,ãfãã,ãf«ãf¼ãã,¿ã€Žroutersã⚡ã,éã,æššã⚡—ã⚡|ã,ã⚡·ã⚡,,ã€,
3. è£½ã"ã,»ãf-ã,¯ã,¿ã⚡@ã⚡³ã⚡@ãfšãã,µãf³ã⚡<ã,%oç%o¹ã@šã⚡@ãf«ãf¼ãã,¿ãf·ãã,ãfãfãf¼ãã,'éã⚡
4. è£½ã"ã,»ãf-ã,¯ã,¿ã⚡@ã⚡³ãfšãã,µãf³ã⚡<ã,%oç%o¹ã@šã⚡@è£½ã"ã,'éã,æššã⚡—ã⚡¾ã⚡™ã€
5. ã,ãfãf¼ãã,· > IOS XR ã,½ãf·ãfãã,ã,šã,çãf;ãf³ãf†ãfšãf³ãã,¹ã,çãfãfãf—ãf†ãf¼ãf¹¼SMUi¼%oã⚡š- 6.5.3ã€ŽSoftwareã⚡ã,éã,æššã⚡—ã⚡|ã,ã⚡·ã⚡,,ã€,
6. ã€CEsshãµf¼ãfã netconfã€ã⚡@ã,ããšãfãfãfããf-ã,¹ã,ããf-ã,ãfšãf³ã⚡@ SMUã⚡ã⚡@ãf€ã,|ãf³ãfãf¼ãf%oãfãf³ãã,¯ã,'ã€ACLã¥ãã⚡-ã⚡—ã⚡¾ã⚡ã>ã,"ã⚡šã⚡—ã⚡Ýãš¹æžœãf³ãfãf¼ãã,¹ã,'ã,¯ãf³ãfãfãã,¯ã⚡—ã⚡|ã,ã⚡·ã⚡,,ã€,

SMU

ã⚡CEã¿...é^ãf—ãf@ãfãfãfããfãã,©ãf¼ãfã⚡@ã⚡ã⚡Ýã,ã⚡ã⚡«ãfãã,¹ãfãã⚡·ã,CEã⚡|ã⚡,,ã⚡ã⚡ã⚡,,ã'ãããããã SMUã,'è|ã⚡æ±,ã⚡™ãã,ã⚡ããã,ã⚡ã⚡ã,çã,«ã,|ãf³ãfããfãfãfããã< Cisco TACã⚡«é€£çµ;ã⚡—ã⚡|ã,ã⚡·ã⚡,,ã€,

ã,ã€£ã^©ç"ã°ã¾ãã⚡ã...ã¼ãç™ºè;™

Cisco Product Security Incident Response

Teami¼PSIRTi¼%oã⚡šã⚡ã€æœ-ã,çãf%oããfãã,µã,¶ãfããã«è~è¼%oã⚡·ã,CEã⚡|ã⚡,,ã,è,,†ã¼±æ€

ã†°ã...

ã⚡"ã⚡@è,,†ã¼±æ€šã⚡ã€Cisco TACã⚡@ã,µãfããf¼ãfãã,±ãf¼ãã,¹ã⚡@èš£æ±°ãã⚡«ç™ºè|ã⚡·ã,CEã⚡¾ã⚡—ã⚡ããã,

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191120-iosxr-ssh-bypass>

æ"¹è,,ã±¥æ'

ã€™

ãfãf¼ãã,ãfšãf³	èª-æžš	
1.1	clarifiedãf³ãfãf¼ãã,¹ã⚡«è²ã½"ã⚡—ã⚡¾ã⚡—ã⚡ããã, SMUã,'è ã⚡æ±,ã⚡™ãã,ã⚡ããã,ã⚡ã⚡@è;½ãšã⚡·ã,CEã⚡ããæ%o<é†ã€,ã€CEè,,†ã¼±æ€šã⚡	

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。