

Cisco IOS XE **Web UI** **Denial of Service** Vulnerability



Severity: Medium
Product: Cisco IOS XE Web UI
Version: 17.3.1
CVSS: 6.5
Workarounds: No workarounds available
Cisco ID: CSCw76009

[CVE-2023-20066](#)

Summary: A Denial of Service (DoS) vulnerability exists in the Cisco IOS XE Web UI. An attacker can exploit this vulnerability to cause a denial of service on the affected device.

Impact:

Cisco IOS XE **Web UI**

UI **Denial of Service** vulnerability exists in the Cisco IOS XE Web UI. An attacker can exploit this vulnerability to cause a denial of service on the affected device.

UI **Denial of Service** vulnerability exists in the Cisco IOS XE Web UI. An attacker can exploit this vulnerability to cause a denial of service on the affected device.

Workarounds: No workarounds are available.

UI **Denial of Service** vulnerability exists in the Cisco IOS XE Web UI. An attacker can exploit this vulnerability to cause a denial of service on the affected device.

UI **Denial of Service** vulnerability exists in the Cisco IOS XE Web UI. An attacker can exploit this vulnerability to cause a denial of service on the affected device.
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtv-es7GSb9V>

UI **Denial of Service** vulnerability exists in the Cisco IOS XE Web UI.

UI **Denial of Service** vulnerability exists in the Cisco IOS XE Web UI. An attacker can exploit this vulnerability to cause a denial of service on the affected device.
[Event Response: March 2023 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication](#)

References:

è,†å¼±æ€šã®ã,ã,è£½å”

å...¬é¬æ™,ç,1ãšã¬ã€ãã“ã®è,,†å¼±æ€šã¬Cisco IOS

XEã,½ãf•ãf^ã,|ã,šã,çãšWeb

UIã©æœ%ãš1ã«ãªã£ã|ã,,ã,ã´ã^ã«ã½±éÿã,´ã—ã´ã¼ã—ãÿã€,

å...¬é¬æ™,ç,1ãšã,,†å¼±æ€šã©çç°èªã•ã,ã,ã|ã,,ã, Cisco

ã,½ãf•ãf^ã,|ã,šã,çã®ãfªãfªãf¼ã,1ã«ãªã,,ã|ã¬ã€ãã“ã®ã,çãf%ããfã,ãã,¶ãfªã®

HTTP ã,¶f¼ãfè”ãšã®çç°èª

ã,ã,ãfªãfã,ãã,1ãš HTTP

ã,µãf¼ãfã©æœ%ãš1ã¬ã©ã¬ã¬ã,´ã^æ¬ã™ã,ãã¬ã¬ã¬ãfªãfã,ãã,1ã«ãfã,°ã,ã

ãš show running-config| include ip http server|secure|active

ã,³ãfžãf³ãf%ãã,´ã½ç”ã—ã|ã€ã,°ãfãf¼ãfãf«

ã,³ãf³ãfã,£ã,®ãfªãf¬ãf¼ã,ãfšãf³ã« ip http server ã,³ãfžãf³ãf%ã¼ãÿã¬ ip

http secure-server

ã,³ãfžãf³ãf%ãã©ã,ã,ã¬ã¬ã©ã¬ã¬ã,´çç°èªã—ã¼ã™ã€, | include ip http

server|secure|activeã,³ãfžãf³ãf%ãã,´ã½ç”ã—ã|ã€ã,°ãfãf¼ãfãfã«ã,³ãf³ãfã,£ã,®ãfªãf¬ãf¼ã,ã

http serverã,³ãfžãf³ãf%ã¼ãÿã¬ ip http secure-

serverã,³ãfžãf³ãf%ãã©ã~ãœ”ã¬ã™ã,ãã¬ã¬ã©ã¬ã¬ã,´çç°èªã—ã¼ã™ã€,ã,,ãšã,ã

ã»ÿã,ã«ãš show running-config | include ip http

server|secure|activeã,³ãfžãf³ãf%ãã,´ç™°è;ã—ã¼ã™ã€,

<#root>

Router#

show running-config | include ip http server|secure|active

ip http server

ip http secure-server

æ³´¼šãfªãfã,ãã,1è”ãšã«ã,,ãšã,ã,ã®ã,³ãfžãf³ãf%ã¼ãÿãÿã¬ã,æ¬1ã®ã,³ãfžãf³ã

UIæ©ÿèf½ã©æœ%ãš1ã«ãªã£ã|ã,,ã¼ã™ã€,

ip http server ã,³ãfžãf³ãf%ãã©ã~ãœ”ã—ã€è”ãšã« ip http active-session-modules none

ã,,ã«ã¼ã,ã,ã|ã,,ã,ã´ã^ã€è,,†å¼±æ€šã© HTTP

çµç”±ãšã,¬ã,¬ã,1ãf—ãfã,ããf^ã•ã,ã,ã¬ãã“ã¬ã¬ã,ã,šã¼ã»ã,“ã€,

Ip http secure-server

æ''¹è'',å±¥æ´

ãf◊ãf¼ã,ãfšãf³	èª-æ~Ž	ã,»ã,ã,ãfšãf³	ã,¹ãf†ãf¼ã,¿ã,¹	æ—¥ä»~
1.0	å^◊å>žå...-é-<ãfªãfªãf¼ã,¹	-	Final	2023å¹³æœ²2æ—¥

å^©ç''è!◊ç´,,

æœ-ã,çãf%ãf◊ã,ã,ã,ãfªã◊ç,,;à¿◊è''¼ã◊@ã,,ã◊@ã◊ã◊-ã◊|ã◊"æ◊◊ã¾ã◊-ã◊|ã◊Šã,Šã€
æœ-ã,çãf%ãf◊ã,ã,ã,ãfªã◊@æf...å±ã◊Šã,^ã◊³ãfªãf³ã,ã◊@ã½¿ç''ã◊«é-çã◊™ã,<è²-ã»ã◊@ã,€
ã◊¾ã◊ÿã€◊ã,ã,¹ã,³ã◊-æœ-ãf%ã,ãf¥ãf;ãf³ãf^ã◊@å†...å@¹ã,'ã^å'Sã◊ªã◊-ã◊«åª%ãæ'ã◊-ã◊
æœ-ã,çãf%ãf◊ã,ã,ã,ãfªã◊@è''è¿å†...å@¹ã◊«é-çã◊-ã◊|æf...å±é...◊ä¿jã◊@ URL
ã,'çœ◊ç•¥ã◊-ã€◊å◊~ç<-ã◊@è»çè¼%ã,,æ,,◊è''³ã,'æ-½ã◊-ã◊ÿã'å◊^ã€◊å½"çª¾ã◊CEç@;ç◊
ã◊"ã◊@ãf%ã,ãf¥ãf;ãf³ãf^ã◊@æf...å±ã◊-ã€◊ã,ã,¹ã,³è£½å"◊ã◊@ã,ãf³ãf%ãf|ãf¼ã,ã,ã,¹ã¾è±;ã

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。