

Cisco IOS XE Denial of Service



Cisco IOS XE Denial of Service ID : cisco-sa-20170927-ios-xe

[CVE-2017-12222](#)

Published : 2017-09-27 16:00

Version : 1.0 : Final

CVSS Score : 7.4

Workarounds : No workarounds available

Cisco ID : [CSCvd45069](#)

Denial of Service (DoS) vulnerability in Cisco IOS XE routers and switches.

Impact

Cisco IOS XE routers and switches are affected by a Denial of Service (DoS) vulnerability.

The vulnerability is located in the `show ip interface` command.

The vulnerability is caused by a buffer overflow in the `show ip interface` command. An attacker can exploit this vulnerability by sending a specially crafted request to the affected device. This request causes the device to crash and become unavailable.

The vulnerability is present in Cisco IOS XE versions 15.2(2)M and earlier.

The vulnerability is present in Cisco IOS XE versions 15.2(2)M and earlier. The vulnerability is present in Cisco IOS XE versions 15.2(2)M and earlier.

The vulnerability is present in Cisco IOS XE versions 15.2(2)M and earlier.

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-ios-xe>

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Denial of Service (DoS) vulnerability in Cisco IOS XE routers and switches.

ä, æ£â^©ç''' ä°<ä¾<ã ♦ " å...-å¼♦ç™°èj''

Cisco Product Security Incident Response

Teami¼^PSIRTi¼%õ ♦ Šã ♦ -ã€ ♦ æœ-ã, çãf%õãf ♦ ã, ðã, ¶ãfã ♦ «è''~è¼%õã ♦ •ã, ÇEã ♦ |ã ♦ ,,ã, <è,, tå¼±æ€

å±°å... ,

ã"ã ♦ ®è,, tå¼±æ€Šã ♦ -ã, µãf ♦ ãf¼ãf^

ã, ±ãf¼ã, 1ã ♦ ®èš£æ±°ã, ã ♦ «ç™°è | <ã ♦ •ã, ÇEã ♦ ¾ã ♦ -ã ♦ Ÿã€,

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-ios-xe>

æ''1è'', å±Ÿæ´

â€''

Version	Description	Section	Status	æ—Ÿã»~
1.0	å^ ♦ å>žå...-é-<ãfãfãf¼ã, 1		Final	2017 å¹´ 9 æœ^ 27 æ—Ÿ

å^©ç'''è! ♦ ç´ ,,

æœ-ã, çãf%õãf ♦ ã, ðã, ¶ãfã ♦ -ç,, jãz ♦ è''¼ã ♦ ®ã,, ã ♦ ®ã ♦ "ã ♦ -ã ♦ |ã ♦ "æ ♦ ♦ ã¾>ã ♦ -ã ♦ |ã ♦ Šã, Šã€
æœ-ã, çãf%õãf ♦ ã, ðã, ¶ãfã ♦ ®æf...å ±ã ♦ Šã, ^ã ♦ ¾ãfãf¾ã, -ã ♦ ®ã¼çç'''ã ♦ «é-çã ♦ ™ã, <è²-ã»ã ♦ ®ã, €
ã ♦ ¾ã ♦ Ÿã€ ♦ ã, ã, 1ã, ¾ã ♦ -æœ-ãf%õã, ãfãf;ãf¾ãf^ã ♦ ®å t...å ®1ã, 'ã °ã Šã ♦ ãã ♦ -ã ♦ «å±°æ>ã ♦ -ã ♦
æœ-ã, çãf%õãf ♦ ã, ðã, ¶ãfã ♦ ®è''~è¼°å t...å ®1ã ♦ «é-çã ♦ -ã ♦ |æf...å ±é... ♦ äzjã ♦ ® URL
ã, çœ ♦ ç´•ã ♦ -ã € ♦ å ♦ ~ç<-ã ♦ ®è»çè¼%õã,, æ,, è''¾ã, æ-½ã ♦ -ã ♦ Ÿã ´ã ♦ ^ã € ♦ å¼"ç¾¾ã ♦ Çç®;ç ♦
ã ♦ "ã ♦ ®ãf%õã, ãfãf;ãf¾ãf^ã ♦ ®æf...å ±ã ♦ -ã € ♦ ã, ã, 1ã, ¾è£½å" ♦ ã ♦ ®ã, "ãf¾ãf%õãf |ãf¼ã, ¶ã, å¾±;

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。