

Catalyst 9000 **SNMPv3** Cisco IOS XE **DoS**



Cisco Catalyst 9000 **SNMPv3 Cisco IOS XE **DoS****
ID : cisco-sa-
iosxe-ewlc-snmp-dos-wNkedg9K
Date : 2020-09-24 16:00
Version : Final
CVSS : [7.4](#)
Impact : Yes
Cisco ID : [CSCvs56562](#)

[CVE-2020-3390](#)

SNMPv3 Cisco IOS XE **DoS**

Summary

Cisco Catalyst 9000 **SNMPv3** Cisco IOS XE **DoS** Simple Network Management Protocol (SNMP) is a widely used protocol for network management. This vulnerability affects the **SNMPv3** implementation in Cisco Catalyst 9000 series switches running Cisco IOS XE.

The vulnerability is a Denial of Service (DoS) attack that can be triggered by sending a specially crafted SNMPv3 message to the affected device. The attack exploits a buffer overflow in the SNMPv3 implementation, leading to a crash of the device's management plane.

The attack is triggered by sending a specially crafted SNMPv3 message to the affected device. The attack exploits a buffer overflow in the SNMPv3 implementation, leading to a crash of the device's management plane.

The attack is triggered by sending a specially crafted SNMPv3 message to the affected device. The attack exploits a buffer overflow in the SNMPv3 implementation, leading to a crash of the device's management plane.

The attack is triggered by sending a specially crafted SNMPv3 message to the affected device. The attack exploits a buffer overflow in the SNMPv3 implementation, leading to a crash of the device's management plane.

The attack is triggered by sending a specially crafted SNMPv3 message to the affected device. The attack exploits a buffer overflow in the SNMPv3 implementation, leading to a crash of the device's management plane.

The attack is triggered by sending a specially crafted SNMPv3 message to the affected device. The attack exploits a buffer overflow in the SNMPv3 implementation, leading to a crash of the device's management plane.

The attack is triggered by sending a specially crafted SNMPv3 message to the affected device. The attack exploits a buffer overflow in the SNMPv3 implementation, leading to a crash of the device's management plane.

Cisco IOS 3.13.8S, 3.13.8S IOS XE

3.13.8S, 3.13.8S IOS XE
Cisco Software Checker

3.13.8S, 3.13.8S IOS XE
3.13.8S, 3.13.8S IOS XE

3.13.8S, 3.13.8S IOS XE
Fixed 3.13.8S, 3.13.8S IOS XE

3.13.8S, 3.13.8S IOS XE
First Fixed 3.13.8S, 3.13.8S IOS XE

[Cisco Software Checker](#)

[3.13.8S, 3.13.8S IOS XE](#)

- 3.13.8S, 3.13.8S IOS XE
- 3.13.8S, 3.13.8S IOS XE
- show version 3.13.8S, 3.13.8S IOS XE

3.13.8S, 3.13.8S IOS XE
3.13.8S, 3.13.8S IOS XE

3.13.8S, 3.13.8S IOS XE

3.13.8S, 3.13.8S IOS XE

3.13.8S, 3.13.8S IOS XE

3.13.8S, 3.13.8S IOS XE

[Cisco Software Checker](#) [Security Impact Rating](#)

3.13.8S, 3.13.8S IOS XE
Cisco Software Checker

3.13.8S, 3.13.8S IOS XE

[3.13.8S, 3.13.8S IOS XE]

3.13.8S, 3.13.8S IOS XE [Medium]

3.13.8S, 3.13.8S IOS XE

Cisco IOS XE 3.13.8S, 3.13.8S IOS XE

3.13.8S, 3.13.8S IOS XE

3.13.8S, 3.13.8S IOS XE [Cisco IOS XE 2 Release](#)

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。