

Cisco IOS XE, Cisco NX-OS, Cisco IOS of Service (DoS) CVE-2020-3228



Medium
 CVE ID : [cisco-sa-sxp-68TEVzR](https://cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sxp-68TEVzR) [CVE-2020-3228](https://cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sxp-68TEVzR)
 Published : 2020-06-03 16:00
 Version : 1.0 : Final
 CVSS Score : 6.8
 Workarounds : No workarounds available
 Cisco ID : [CSCvt30182](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sxp-68TEVzR) [CSCvd71220](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sxp-68TEVzR)
[CSCvp96954](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sxp-68TEVzR)

Cisco IOS XE, Cisco NX-OS, Cisco IOS of Service (DoS) CVE-2020-3228

Summary

Cisco IOS XE, Cisco NX-OS, Cisco IOS of Service (DoS) CVE-2020-3228 is a Denial of Service (DoS) vulnerability in Cisco IOS XE, Cisco NX-OS, and Cisco IOS of Service (DoS) versions 15.6(3) and later. The vulnerability exists in the Security Group Tag Exchange Protocol (SXP) and can be exploited by sending specially crafted packets to the affected devices. The impact is a Denial of Service (DoS) condition that causes the affected devices to crash or become unresponsive. The CVSS score is 6.8, indicating a medium level of severity. No workarounds are available. The vulnerability is tracked by Cisco under the IDs CSCvt30182, CSCvd71220, and CSCvp96954. For more information, see the [Cisco Security Advisory](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sxp-68TEVzR).

Impact

The impact of this vulnerability is a Denial of Service (DoS) condition that causes the affected devices to crash or become unresponsive. The affected devices are Cisco IOS XE, Cisco NX-OS, and Cisco IOS of Service (DoS) versions 15.6(3) and later. The vulnerability is tracked by Cisco under the IDs CSCvt30182, CSCvd71220, and CSCvp96954. For more information, see the [Cisco Security Advisory](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sxp-68TEVzR).

Security

Advisory [Cisco Software Checker](#) [Security Impact Rating](#) [Cisco IOS XE 2 Release Notes](#) [Cisco IOS XE 3S Release Notes](#) [Cisco NX-OS 3.4](#)

[Cisco Software Checker](#) [Security Impact Rating](#) [Cisco IOS XE 2 Release Notes](#) [Cisco IOS XE 3S Release Notes](#) [Cisco NX-OS 3.4](#)

[Cisco IOS XE 2 Release Notes](#) [Cisco IOS XE 3S Release Notes](#) [Cisco NX-OS 3.4](#)

[Cisco IOS XE 2 Release Notes](#) [Cisco IOS XE 3S Release Notes](#) [Cisco NX-OS 3.4](#)

Cisco NX-OS 3.4

[Cisco NX-OS 3.4](#)

[Cisco NX-OS 3.4](#) [Cisco Software Checker](#) [Security Impact Rating](#) [Cisco IOS XE 2 Release Notes](#) [Cisco IOS XE 3S Release Notes](#) [Cisco NX-OS 3.4](#)

[Cisco Software Checker](#)

[Cisco NX-OS 3.4](#) [Cisco Software Checker](#) [Security Impact Rating](#) [Cisco IOS XE 2 Release Notes](#) [Cisco IOS XE 3S Release Notes](#) [Cisco NX-OS 3.4](#)

- [Cisco NX-OS 3.4](#) [Cisco Software Checker](#) [Security Impact Rating](#) [Cisco IOS XE 2 Release Notes](#) [Cisco IOS XE 3S Release Notes](#) [Cisco NX-OS 3.4](#)
- [Cisco NX-OS 3.4](#) [Cisco Software Checker](#) [Security Impact Rating](#) [Cisco IOS XE 2 Release Notes](#) [Cisco IOS XE 3S Release Notes](#) [Cisco NX-OS 3.4](#)
- [Cisco NX-OS 3.4](#) [Cisco Software Checker](#) [Security Impact Rating](#) [Cisco IOS XE 2 Release Notes](#) [Cisco IOS XE 3S Release Notes](#) [Cisco NX-OS 3.4](#)

[Cisco NX-OS 3.4](#) [Cisco Software Checker](#) [Security Impact Rating](#) [Cisco IOS XE 2 Release Notes](#) [Cisco IOS XE 3S Release Notes](#) [Cisco NX-OS 3.4](#)

Cisco NX-OS 7.0(3)I7(5) 14.0(1h)

Cisco NX-OS 7.0(3)I7(5) 14.0(1h)

Cisco Software Checker Security Impact Rating

Cisco Product Security Incident Response

Team PSIRT

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sxp-68TEVzR>

Table

Table with 5 columns: Version, Description, Status, Date, and Reference

Table

Version	Description	Status	Date	Reference
1.0	Final		2020 06 03	

Table

Table with 5 columns: Version, Description, Status, Date, and Reference

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。