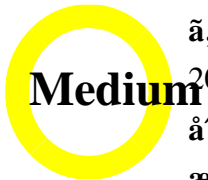


Cisco NX-

OS (Cisco NX-OS 7.0(3)IY(1) [1783])



Cisco Security Advisory ID : cisco-sa-20190515-nxos-cmdinj-1783

[CVE-2019-1783](#)

Published : 2019-05-15 16:00

Last Updated : 2019-07-18 00:00

Version : 1.1 : Final

CVSS Score : [6.7](#)

Workarounds : No workarounds available

Cisco Bug ID : [CSCvi42281](#) [CSCvj03966](#)

Summary: A Denial of Service (DoS) vulnerability exists in the Cisco NX-OS CLI. An attacker can exploit this vulnerability by sending a specially crafted command to the device, which causes the device to crash and become unavailable.

Details

Cisco NX-

OS (Cisco NX-OS 7.0(3)IY(1) [1783])

A Denial of Service (DoS) vulnerability exists in the Cisco NX-OS CLI. An attacker can exploit this vulnerability by sending a specially crafted command to the device, which causes the device to crash and become unavailable.

The vulnerability is caused by a buffer overflow in the CLI parser. The parser does not properly validate the length of the command string, allowing an attacker to send a command that is longer than the buffer can handle. This causes the parser to overwrite memory, leading to a crash.

CVSS Score: 6.7 (Medium)

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-cmdinj-1783>

Impact

Denial of Service (DoS)

Affected Products: Cisco NX-OS

Impact: A Denial of Service (DoS) attack can be performed against the affected devices, causing them to become unavailable.

- Nexus 5500 (Cisco NX-OS 7.0(3)IY(1) [1783])
- Nexus 5600 (Cisco NX-OS 7.0(3)IY(1) [1783])
- Nexus 6000 (Cisco NX-OS 7.0(3)IY(1) [1783])

[Cisco MDS](#)

[VMware](#)

[Cisco Nexus 3000](#)

[Cisco Nexus 5000 Series Switches](#)

[Cisco Nexus 5500](#)

[Cisco Nexus 6000 Series Switches](#)

[Cisco Nexus 7000 Series Switches](#)

[Cisco Nexus 9000 Series Switches](#)

[ACI](#)

[Cisco UCS](#)

[Cisco NX-OS](#)

[Cisco Product Security Incident Response Team](#)

[Cisco Product Security Incident Response Team](#)

[Cisco Product Security Incident Response Team](#)

[Cisco Product Security Incident Response Team](#)

[Cisco Product Security Incident Response Team](#)

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-cmdinj-1783>

[Cisco Product Security Incident Response Team](#)

Cisco Product Security Incident Response Team	Cisco Product Security Incident Response Team	Cisco Product Security Incident Response Team
1.1	Nexus 7000/7700	Cisco Product Security Incident Response Team
1.0	Cisco Product Security Incident Response Team	-

[Cisco Product Security Incident Response Team](#)

[Cisco Product Security Incident Response Team](#)

ã¼ãÿã€ã,ã,¹ã³ãæœ-ãf%ã,ãfãfjãf³ãf^ã®ãt...ã®¹ã,'ã^ã'šãªã—ã«ã%ãæ'ã—ã
æœ-ã,ããf%ããfãã,ãã,ããfãã®è"~è¿ãt...ã®¹ã«é-ãã—ã!æf...ã±é...ã¿jã® URL
ã,¿œ¿•ã—ã€ãã¿ç<-ã®è»¿è¼%ã,,æ,,è"³ã,'æ-½ã—ãÿã'ã^ã€ã½"¿¾ãœç®jç
ã"ã®ãf%ã,ãfãfjãf³ãf^ã®æf...ã±ãæ-ã,ã,¹ã,³è½ã"ã®ã,"ãf³ãf%ããf!ãf¼ã,ã,ã³¼è±jã

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。