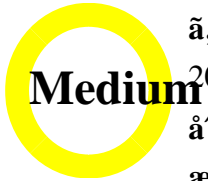


# Cisco

## Nexus OS 1000V, 3000 Series, and 3500 Series Switches CLI Command Injection Vulnerability



Cisco-Security-ID : cisco-sa-

[CVE-2017-](#)

20170517-nss

[6649](#)

Published: 2017-05-17 16:00

Updated: 2017-10-19 17:02

Version: 1.2 : Final

CVSS Score: 4.4

Workarounds: No workarounds available

Cisco Bug IDs: [CSCve60516](#) [CSCve60555](#)

[CSCvb86787](#) [CSCve62810](#)

A remote attacker can execute arbitrary commands on affected devices by sending a specially crafted CLI command.

### Vulnerability Details

Cisco Nexus OS 1000V, 3000 Series, and 3500 Series Switches are vulnerable to a remote command injection vulnerability. The vulnerability is caused by a flaw in the command line interface (CLI) parser. An attacker can exploit this vulnerability by sending a specially crafted CLI command that contains a shell metacharacter (such as `&#x26;` or `&#x27;`) followed by a command to execute arbitrary code on the device.

The vulnerability affects the following Cisco Nexus OS versions:

- 1000V Series Switches: 6.2(1) and 6.2(2)
- 3000 Series Switches: 7.0(3) and 7.0(4)
- 3500 Series Switches: 7.0(3) and 7.0(4)

The vulnerability is rated as Medium severity (CVSS score of 4.4).

For more information, please refer to the [Cisco Security Advisory](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-nss).

### Workarounds

Upgrade the affected devices to the latest software version.

Alternatively, you can configure the device to restrict access to the CLI command line.

For more information, please refer to the [Cisco Security Advisory](#).

Cisco Nexus 1000V Series Switches

Cisco Nexus 3000 Series Switches

Cisco Nexus 3500 Series Switches



æœ-è,,†â¼±æ€§ã-ã€ã,ã,1ã,³â†...éf-ãšã®ã,»ã,ãfãfãftã,£ãftã,1ãf^ã«ã,^ã£ã|ç™ºè|ã•ã,£ã¾ã-ãÿã€,

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-nss>

æ”¹è,å±ÿæ’

ãfãf¼ã,ãfšãf³	èª-æŽ	ã,»ã
1.2	è,,†â¼±æ€§ãªè£½ã”ã®ãfã,1ãf^ã«Nexus 1000Vã,è½ãšã€,	è,,†â¼±æ€§ã£ã
1.1	è,,†â¼±æ€§ã£ã~ãœ”ã™ã,«è£½ã”ã®ãfã,1ãf^ã,æ’æ-ã€,	è,,†â¼±æ€§ã£ã
1.0	ã^ãžã...-é-ãfãfãf¼ã,¹	-

ã^©ç”¹è!ç’,,

æœ-ã,çãf%ãfã,ã,ã,¶ãfãç,,jäçèè¼ã®ã,,ã®ã”ã-ã|ã”æã¾ã-ã|ãšã,šã€æœ-ã,çãf%ãfã,ã,ã,¶ãfã®æf...ã±ãšã,^ã³ãfãfã,ã®ã½ç””ã«é-çã™ã,«è²-ã»ã®ã,ã¾ãÿã€ã,ã,1ã,³ã-æœ-ãf%ã,ãfãfãfãfã®ã†...ã®¹ã,’ã^ãšãªã-ã«ã%ãæ’ã-ãæœ-ã,çãf%ãfã,ã,ã,¶ãfã®è~èç°â†...ã®¹ã«é-çã-ã|æf...ã±é...ãçjã® URLã,’çœçç¥ã-ã€ã~ç<-ã®è»çè¼%ã,,æ,,è³ã,’æ-½ã-ãÿã’ã^ã€ã½”ç¾ã£ç®ççã”ã®ãf%ã,ãfãfãfãfã®æf...ã±ã-ã€ã,ã,1ã,³è£½ã”ã®ã,ãfãf%ãf!ãf¼ã,¶ã,ã¾ãè±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。