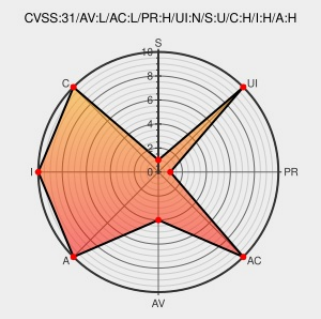
CVE-2018-15368

Published on: 10/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:27 PM UTC

CVE-2018-15368 - advisory for cisco-sa-20180926-privesc

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ios Xe from Cisco contain the following vulnerability:

A vulnerability in the CLI parser of Cisco IOS XE Software could allow an authenticated, local attacker to gain access to the underlying Linux shell of an affected device and execute arbitrary commands with root privileges on the device. The vulnerability is due to the affected software improperly sanitizing command arguments to prevent modifications to the underlying Linux filesystem on a device. An attacker who has privileged EXEC mode (privilege level 15) access to an affected device could exploit this vulnerability on the device by executing CLI commands that contain crafted arguments. A successful exploit could allow the attacker to gain access to the underlying Linux shell of the affected device and execute arbitrary commands with root privileges on the device.

CVE-2018-15368 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Cisco** - **Cisco IOS XE Software** version **n/a**

CVSS3 Score: 6.7 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

COMPLETE | COMPLETE | COMPLETE

CVE References

Description	Tags	Link
Cisco IOS XE Software Privileged EXEC Mode Root Shell Access Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20180926 Cisco IOS XE Software Privileged EXEC Mode Root Shell Access Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios Xe	15.4(3)s	All	All	All
Operating System	Cisco	Ios Xe	15.4\(3\)s	All	All	All
Operating System	Cisco	Ios Xe	15.4\(3\)s	All	All	All

cpe:2.3:o:cisco:ios_xe:15.4(3)s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:15.4\(3\)s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:15.4\(3\)s:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→