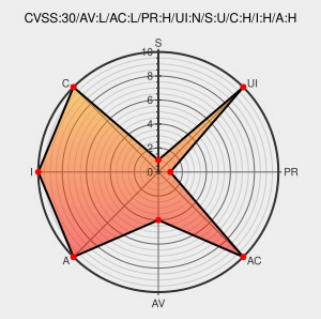
CVE-2018-15371

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

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

CVE-2018-15371 - advisory for cisco-sa-20180926-shell-access

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



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

A vulnerability in the shell access request mechanism of Cisco IOS XE Software could allow an authenticated, local attacker to bypass authentication and gain unrestricted access to the root shell of an affected device. The vulnerability exists because the affected software has insufficient authentication mechanisms for certain commands. An attacker could exploit this vulnerability by requesting access to the root shell of an affected device, after the shell access feature has been enabled. A successful exploit could allow the attacker to bypass authentication and gain unrestricted access to the root shell of the affected device.

CVE-2018-15371 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 Shell Access Authentication Bypass Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20180926 Cisco IOS XE Software Shell Access Authentication Bypass Vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	16.3(1)	All	All	All
Operating System	Cisco	Ios Xe	16.3\(1\)	All	All	All
Operating System	Cisco	Ios Xe	16.3\(1\)	All	All	All

cpe:2.3:o:cisco:ios_xe:16.3(1):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.3\(1\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.3\(1\):*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→