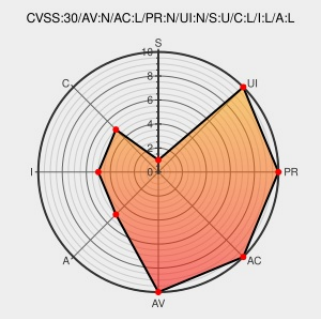
CVE-2016-6474

Published on: 12/13/2016 12:00:00 AM UTC

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

CVE-2016-6474

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



Certain versions of Ios from Cisco contain the following vulnerability:

A vulnerability in the implementation of X.509 Version 3 for SSH authentication functionality in Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to bypass authentication on an affected system. More Information: CSCuv89417. Known Affected Releases: 15.5(2.25)T. Known Fixed Releases: 15.2(4)E1 15.2(4)E2 15.2(4)E3 15.2(4)EA4 15.2(4.0r)EB 15.2(4.1.27)EB 15.2(4.4.2)EA4 15.2(4.7.1)EC 15.2(4.7.2)EC 15.2(5.1.1)E 15.2(5.5.63)E 15.2(5.5.64)E 15.4(1)IA1.80 15.5(3)M1.1 15.5(3)M2 15.5(3)S1.4 15.5(3)S2 15.6(0.22)S0.12 15.6(1)T0.1 15.6(1)T1 15.6(1.15)T 15.6(1.17)S0.7 15.6(1.17)SP 15.6(1.22.1a)T0 15.6(2)S 15.6(2)SP 16.1(1.24) 16.1.2 16.2(0.247) 16.3(0.11) 3.8(1)E Denali-16.1.2.

CVE-2016-6474 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.3 - HIGH

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

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco IOS and IOS XE Software SSH X.509 Authentication Bypass Vulnerability	Mitigation Vendor Advisory tools.cisco.com text/html	CONFIRM tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-ios-xe-x509
Cisco IOS/IOS XE Lets Remote Users Bypass Authentication on the Target System - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1037420
Cisco IOS and IOS XE Software CVE-2016-6474 Authentication Bypass Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 94773

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	15.5(2.25)t	All	All	All
Operating System	Cisco	Ios	15.5\(2.25\)t	All	All	All
Operating System	Cisco	Ios	15.5\(2.25\)t	All	All	All

cpe:2.3:o:cisco:ios:15.5(2.25)t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.5\(2.25\)t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.5\(2.25\)t:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→