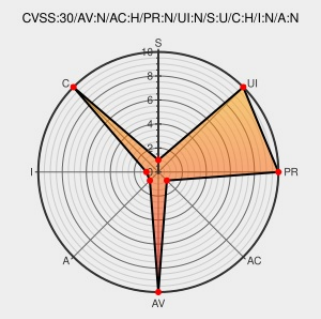
CVE-2011-4667

Published on: 09/25/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:12 PM UTC

CVE-2011-4667

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



Certain versions of Ios from Cisco contain the following vulnerability:

The encryption library in Cisco IOS Software 15.2(1)T, 15.2(1)T1, and 15.2(2)T, Cisco NX-OS in Cisco MDS 9222i Multiservice Modular Switch, Cisco MDS 9000 18/4-Port Multiservice Module, and Cisco MDS 9000 Storage Services Node module before 5.2(6), and Cisco IOS in Cisco VPN Services Port Adaptor for Catalyst 6500 12.2(33)SXI, and 12.2(33)SXJ when IP Security (aka IPSec) is used, allows remote attackers to obtain unencrypted packets from encrypted sessions.

CVE-2011-4667 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Cisco Software Encryption Library Information Disclosure Vulnerability	Vendor Advisory tools.cisco.com	CISCO 20120913 Cisco Software Encryption Library Information Disclosure

	text/html	Vulnerability
Release Notes for Cisco IOS Release 12.2SX - Caveats in Release 12.2(33)SXI Rebuilds [Cisco Catalyst 6500 Series Switches] - Cisco	Vendor Advisory www.cisco.com text/html	CISCO 20150825 Chapter: Caveats in Release 12.2(33)SXI Rebuilds

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	12.2(33)sxi	All	All	All
Operating System	Cisco	Ios	12.2(33)sxj	All	All	All
Operating System	Cisco	Ios	12.2\(33\)sxi	All	All	All
Operating System	Cisco	Ios	12.2\(33\)sxj	All	All	All
Operating System	Cisco	Ios	15.2(1)t	All	All	All
Operating System	Cisco	Ios	15.2(1)t1	All	All	All
Operating System	Cisco	Ios	15.2(2)t	All	All	All
Operating System	Cisco	Ios	15.2\(1\)t	All	All	All
Operating System	Cisco	Ios	15.2\(1\)t1	All	All	All
Operating System	Cisco	Ios	15.2\(2\)t	All	All	All
Operating System	Cisco	Ios	12.2\(33\)sxi	All	All	All
Operating System	Cisco	Ios	12.2\(33\)sxj	All	All	All
Operating System	Cisco	Ios	15.2\(1\)t	All	All	All
Operating System	Cisco	Ios	15.2\(1\)t1	All	All	All
Operating System	Cisco	Ios	15.2\(2\)t	All	All	All
Operating System	Cisco	Nx-os	5.0(5)	All	All	All

Operating System	Cisco	Nx-os	5.0\(5\)	All	All	All
Operating System	Cisco	Nx-os	5.0\(5\)	All	All	All

cpe:2.3:o:cisco:ios:12.2(33)sxi:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.2(33)sxj:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.2\(33\)sxi:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.2\(33\)sxj:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2(1)t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2(1)t1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2(2)t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(1\)t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(1\)t1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(2\)t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.2\(33\)sxi:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.2\(33\)sxj:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(1\)t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(1\)t1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(2\)t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:5.0(5):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:5.0\(5\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:5.0\(5\):*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report