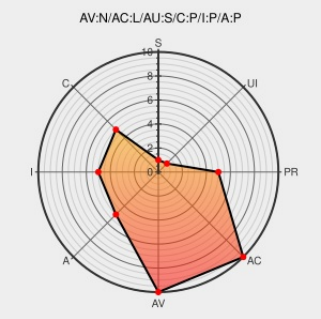
CVE-2014-2130

Published on: 03/05/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:58 PM UTC

CVE-2014-2130

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



Certain versions of Secure Access Control System from Cisco contain the following vulnerability:

Cisco Secure Access Control Server (ACS) provides an unintentional administration web interface based on Apache Tomcat, which allows remote authenticated users to modify application files and configuration files, and consequently execute arbitrary code, by leveraging administrative privileges, aka Bug ID CSCuj83189.

CVE-2014-2130 has been assigned by psirt@cisco.com to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Cisco Secure Access Control Server Tomcat Administration Interface Lets Remote Authenticated Users Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1031844
Cisco Secure Access Control Server Default Tomcat Administration Interface Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20150304 Cisco Secure Access Control Server Default Tomcat Administration Interface Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Secure Access Control System	-	All	All	All
Application	Cisco	Secure Access Control System	-	All	All	All

cpe:2.3:a:cisco:secure_access_control_system:-:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:secure_access_control_system:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→