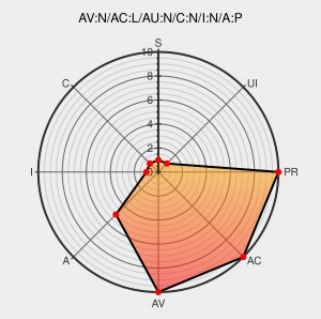
CVE-2013-5536

Published on: 10/24/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:36 PM UTC

CVE-2013-5536

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 System (ACS) does not properly implement an incoming-packet firewall rule, which allows remote attackers to cause a denial of service (process crash) via a flood of crafted packets, aka Bug ID CSCui51521.

CVE-2013-5536 has been assigned by psirt@cisco.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Cisco Security Notice: Cisco Secure ACS Distributed Deployment Denial of Service Vulnerability	Vendor Advisory, tools.cisco.com, text/html	CISCO 20131022 Cisco Secure ACS Distributed Deployment Denial of Service 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→