CVE-2013-5470

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2013-5470
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-09-04 03:24:37 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cisco Secure Access Control System (ACS) does not properly handle requests to read from the TACACS+ socket, which a

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
osvdb.org/96822	af854a3a-2127-422b-91ae-364da2661108
tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-5470	af854a3a-2127-422b-91ae-364da2661108
Cisco Secure Access Control System CVE-2013-5470 Remote Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.