CVE-2011-3293

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

Summary

CVE	CVE-2011-3293
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-05-02 10:09:21 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Multiple cross-site request forgery (CSRF) vulnerabilities in the Solution Engine in Cisco Secure Access Control Server (AC

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-352 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Secure Access Control Server	5.2	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link
www.cisco.com/web/software/282766937/37718/Acs-5-2-0-26-9-Readme.txt	af854a3a-2127-422b-91ae-364da2661108	www.cisco.com
Cisco Secure Access Control System (ACS) Multiple Security Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.securityfocu
About Secunia Research | Flexera	af854a3a-2127-422b-91ae-364da2661108	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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