CVE-2014-0667

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

Summary

CVE	CVE-2014-0667
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-16 19:55:04 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The RMI interface in Cisco Secure Access Control System (ACS) does not properly enforce authorization requirements, wh

Risk And Classification

Primary CVSS: v2.0 6.3 from nvd@nist.gov

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

EPSS: 0.006230000 probability, percentile 0.702200000 (date 2026-05-03)

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

Complete

Integrity

None

Availability

None

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

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
Cisco Secure Access Control Server RMI Interface Lets Remote Users Read Files - SecurityTracker	af854a3a-2127-422b-91ae-364da2661
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661
Cisco Security Notice: Cisco Secure ACS RMI Arbitrary File Read Vulnerability	af854a3a-2127-422b-91ae-364da2661
Alert Details - Security Center - Cisco Systems	af854a3a-2127-422b-91ae-364da2661
osvdb.org/102168	af854a3a-2127-422b-91ae-364da2661
Cisco Secure Access Control System RMI Interface Authorization Bypass Vulnerability	af854a3a-2127-422b-91ae-364da2661
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.