CVE-2014-0648

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

Summary

CVE	CVE-2014-0648
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) 5.x before 5.5 does not properly enforce authentication a

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

EPSS: 0.077780000 probability, percentile 0.919740000 (date 2026-04-29)

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Cisco	Secure Access Control System	5.1	All	All	All
Application	Cisco	Secure Access Control System	5.1.0.44	All	All	All
Application	Cisco	Secure Access Control System	5.1.0.44.1	All	All	All
Application	Cisco	Secure Access Control System	5.1.0.44.2	All	All	All
Application	Cisco	Secure Access Control System	5.1.0.44.3	All	All	All
Application	Cisco	Secure Access Control System	5.1.0.44.4	All	All	All
Application	Cisco	Secure Access Control System	5.1.0.44.5	All	All	All
Application	Cisco	Secure Access Control System	5.2	All	All	All
Application	Cisco	Secure Access Control System	5.2.0.26	All	All	All
Application	Cisco	Secure Access Control System	5.2.0.26.1	All	All	All
Application	Cisco	Secure Access Control System	5.2.0.26.2	All	All	All
Application	Cisco	Secure Access Control System	5.3.0.40.1	All	All	All
Application	Cisco	Secure Access Control System	5.3.0.40.2	All	All	All
Application	Cisco	Secure Access Control System	5.3.0.40.3	All	All	All
Application	Cisco	Secure Access Control System	5.3.0.40.4	All	All	All
Application	Cisco	Secure Access Control System	5.3.0.40.5	All	All	All
Application	Cisco	Secure Access Control System	5.3.0.40.6	All	All	All
Application	Cisco	Secure Access Control System	5.3.0.40.7	All	All	All
Application	Cisco	Secure Access Control System	5.3.0.40.8	All	All	All
Application	Cisco	Secure Access Control System	5.3.0.40.9	All	All	All
Application	Cisco	Secure Access Control System	5.4.0.46.1	All	All	All
Application	Cisco	Secure Access Control System	5.4.0.46.2	All	All	All
Application	Cisco	Secure Access Control System	5.4.0.46.3	All	All	All
Application	Cisco	Secure Access Control System	5.4.0.46.4	All	All	All
Application	Cisco	Secure Access Control System	5.4.0.46.5	All	All	All
Application	Cisco	Secure Access Control System	All	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 System RMI Interface Unauthenticated Access Security Vulnerability	af854a3a-2127-422b-9
Alert Details - Security Center - Cisco Systems	af854a3a-2127-422b-9
Multiple Vulnerabilities in Cisco Secure Access Control System	af854a3a-2127-422b-9

osvdb.org/102117	af854a3a-2127-422b-9
Cisco Secure Access Control Server RMI and Web Interface Bugs Let Remote Users Gain Access - SecurityTracker	af854a3a-2127-422b-9
Security Advisory SA56213 - Cisco Secure Access Control System (ACS) Multiple Vulnerabilities - Secunia	af854a3a-2127-422b-9
IBM X-Force Exchange	af854a3a-2127-422b-9
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.