



CVE-2014-0668

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-0668
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-20 04:58:49 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability in the portal in Cisco Secure Access Control System (ACS) allows remote attackers

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

EPSS: 0.005610000 probability, percentile 0.683970000 (date 2026-05-03)

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/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
osvdb.org/102256						af854a3e
Cisco Secure Access Control Server Input Validation Flaw Permits Cross-Site Scripting Attacks - SecurityTracker						af854a3e
Security Advisory SA56543 - Cisco Secure Access Control System (ACS) Unspecified Cross-Site Scripting Vulnerability - Secunia						af854a3e
IBM X-Force Exchange						af854a3e
Cisco Security Notice: Cisco Secure ACS Portal Cross-Site Scripting Vulnerability						af854a3e
Cisco Secure ACS Portal CVE-2014-0668 Cross Site Scripting Vulnerability						af854a3e
Alert Details - Security Center - Cisco Systems						af854a3e
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.						