



# CVE-2015-6349

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2015-6349
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-10-30 10:59:00 UTC
<b>Updated</b>	2016-12-07 18:19:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in the web interface in the Solution Engine in Cisco Secure Access Control Server (/

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Secure Access Control Server	5.7.0.15	All	All	All
Application	Cisco	Secure Access Control Server	5.7.0.15	All	All	All

## References

Reference	Source
Cisco Secure Access Control Server Input Validation Flaw Lets Remote Conduct Cross-Site Scripting Attacks - SecurityTracker	SECTRACK
Cisco Secure Access Control Server Reflective Cross-Site Scripting Vulnerability	CISCO
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.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**