



CVE-2015-6347

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

Summary

CVE	CVE-2015-6347
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-30 10:59:00 UTC
Updated	2016-12-07 18:19:00 UTC
Description	The Solution Engine in Cisco Secure Access Control Server (ACS) 5.7(0.15) allows remote authenticated users to bypass i

Risk And Classification

Problem Types: CWE-264

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
Cisco Secure Access Control Server Role-Based Access Control URL Lack of Protection Vulnerability
Cisco Secure Access Control Server RBAC Flaw Lets Remote Authenticated Users Modify Dashboard Portlets on the Target System - Securit
CVE Program record
NVD vulnerability detail

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](#)