



CVE-2014-8027

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

Summary

CVE	CVE-2014-8027
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-09 02:59:00 UTC
Updated	2017-09-08 01:29:00 UTC
Description	The RBAC component in Cisco Secure Access Control System (ACS) allows remote authenticated users to obtain Network

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 System	-	All	All	All
Application	Cisco	Secure Access Control System	-	All	All	All

References

Reference	Source	Link
Cisco Secure Access Control Server Lets Remote Authenticated Users Gain Elevated Privileges - SecurityTracker	SECTrack	www.sectrack.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
About Secunia Research Flexera	SECUNIA	secunia.com
Cisco Secure Access Control Server CVE-2014-8027 Privilege Escalation Vulnerability	BID	www.securityfocus.com/bid/67444
20150108 Cisco Secure Access Control Server Privilege Escalation Vulnerability	CISCO	tools.cisco.com/security/center/content/CiscoSecurityAdvisory
CVE Program record	CVE.ORG	www.cve.org/CVE-2014-8027
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2014-8027

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

Free CVE JSON API [cve.report/api](#)

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