



CVE-2014-0651

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2014-0651
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-08 21:55:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	The administrative interface in Cisco Context Directory Agent (CDA) does not properly enforce authorization requirements,

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Context Directory Agent	-	All	All	All
Application	Cisco	Context Directory Agent	-	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	exchange.xf
Cisco Context Directory Agent Remote Privilege Escalation Vulnerability	BID	www.security
101809	OSVDB	osvdb.org
Alert Details - Security Center - Cisco Systems	CONFIRM	tools.cisco.co
Cisco Security Notice: Cisco Context Directory Agent Privilege Escalation Vulnerability	CISCO	tools.cisco.co
Security Advisory SA56365 - Cisco Context Directory Agent Multiple Vulnerabilities - Secunia	SECUNIA	secunia.com
Cisco Context Directory Agent Lets Remote Authenticated Users Take Administrative Actions - SecurityTracker	SECTRACK	www.security
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

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