



CVE-2014-4629

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2014-4629
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-06 15:59:00 UTC
Updated	2018-10-09 19:49:00 UTC
Description	EMC Documentum Content Server 7.0, 7.1 before 7.1 P10, and 6.7 before SP2 P19 allows remote authenticated users to r

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	Documentum Content Server	6.7	All	All	All
Application	Emc	Documentum Content Server	6.7	sp1	All	All
Application	Emc	Documentum Content Server	6.7	sp2	All	All
Application	Emc	Documentum Content Server	7.0	All	All	All
Application	Emc	Documentum Content Server	7.1	All	All	All
Application	Emc	Documentum Content Server	6.7	All	All	All
Application	Emc	Documentum Content Server	6.7	sp1	All	All
Application	Emc	Documentum Content Server	6.7	sp2	All	All
Application	Emc	Documentum Content Server	7.0	All	All	All
Application	Emc	Documentum Content Server	7.1	All	All	All

References

Reference	Source	Link
EMC Documentum Content Server Bug Let Remote Authenticated Users Gain Elevated Privileges - SecurityTracker	SECTRACK	www.se
IBM X-Force Exchange	XF	exchang
EMC Documentum Content Server Insecure Direct Object Reference ≈ Packet Storm	MISC	packets
SecurityFocus	BUGTRAQ	www.se

EMC Documentum Content Server CVE-2014-4629 Remote Privilege Escalation Vulnerability	BID	www.se
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

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