CVE-2014-2513

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-2513
State	PUBLISHED
Assigner	dell
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-08 11:06:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	EMC Documentum Content Server before 6.7 SP1 P28, 6.7 SP2 before P15, 7.0 before P15, and 7.1 before P06 does not

Risk And Classification

Primary CVSS: v2.0 8.2 from nvd@nist.gov

AV:N/AC:M/Au:S/C:C/I:C/A:P

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Partial

AV:N/AC:M/Au:S/C:C/I:C/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	Documentum Content Server	6.7	-	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	All	sp1	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
EMC Documentum Content Server CVE-2014-2513 Remote Privilege Escalation Vulnerability	af854a3a-2127-422b-9
NEOHAPSIS - Peace of Mind Through Integrity and Insight	af854a3a-2127-422b-9
EMC Documentum Content Server Flaws Let Remote Authenticated Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-9
Security Advisory SA59757 - EMC Documentum Content Server Two Security Bypass Vulnerabilities - Secunia	af854a3a-2127-422b-9
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.