CVE-2014-2503

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

Summary

CVE	CVE-2014-2503
State	PUBLISHED
Assigner	dell
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-06 00:55:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The thumbnail proxy server in EMC Documentum Digital Asset Manager (DAM) 6.5 SP3, 6.5 SP4, 6.5 SP5, and 6.5 SP6 be

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	Documentum Digital Asset Manager	6.5	sp3	All	All

Application	Emc	Documentum Digital Asset Manager	6.5	sp4	All	All
Application	Emc	Documentum Digital Asset Manager	6.5	sp5	All	All
Application	Emc	Documentum Digital Asset Manager	6.5	sp6	All	All

Vendor Declared Affected Products

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

References

Reference	Source
archives.neohapsis.com/archives/bugtraq/2014-06/0037.html	af854a3a-212
EMC Documentum Digital Asset Manager CVE-2014-2503 Documentum Query Language Injection Vulnerability	af854a3a-212
EMC Documentum Digital Asset Manager Blind DQL Injection ≈ Packet Storm	af854a3a-212
EMC Documentum Digital Asset Manager Input Validation Flaw Lets Remote Users Inject DQL Commands - SecurityTracker	af854a3a-212
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.