



CVE-2016-9873

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

Summary

CVE	CVE-2016-9873
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-03 07:59:00 UTC
Updated	2017-07-25 01:29:00 UTC
Description	EMC Documentum D2 version 4.5 and EMC Documentum D2 version 4.6 has a DQL Injection Vulnerability that could poten

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	Documentum D2	4.5	All	All	All
Application	Emc	Documentum D2	4.6	All	All	All
Application	Emc	Documentum D2	4.5	All	All	All
Application	Emc	Documentum D2	4.6	All	All	All

References

Reference	Source	Li
SecurityFocus	CONFIRM	w
EMC Documentum D2 Flaw Lets Remote Users Conduct Cross-Site Scripting and DQL Injection Attacks - SecurityTracker	SECTrack	w
EMC Documentum D2 CVE-2016-9873 DQL Injection Vulnerability	BID	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

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](#)