



CVE-2011-0027

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

Summary

CVE	CVE-2011-0027
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-12 01:00:00 UTC
Updated	2023-12-07 18:38:00 UTC
Description	Microsoft Data Access Components (MDAC) 2.8 SP1 and SP2, and Windows Data Access Components (WDAC) 6.0, does

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Data Access Components	2.8	sp1	All	All
Application	Microsoft	Data Access Components	2.8	sp2	All	All
Application	Microsoft	Data Access Components	2.8	sp1	All	All
Application	Microsoft	Data Access Components	2.8	sp2	All	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	All	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	All	All
Operating System	Microsoft	Windows 7	-	All	All	All
Operating System	Microsoft	Windows 7	-	All	All	All
Application	Microsoft	Windows Data Access Components	6.0	All	All	All
Application	Microsoft	Windows Data Access Components	6.0	All	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	x32	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x32	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All

Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	r2	All	itanium	All
Operating System	Microsoft	Windows Server 2008	r2	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	x32	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x32	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	r2	All	itanium	All
Operating System	Microsoft	Windows Server 2008	r2	All	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Xp	All	All	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All
Operating System	Microsoft	Windows Xp	All	All	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All

References
Reference
Repository / Oval Repository
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Vreugdenhil Research » Blog Archive » MS11-002 Pwn2Own heap overflow
Microsoft Data Access Components Two Vulnerabilities - Secunia.com
US-CERT Technical Cyber Security Alert TA11-011A -- Microsoft Updates for Multiple Vulnerabilities
70444
Zero Day Initiative
Microsoft Data Access Components (MDAC) Memory Corruption Errors in Processing DSN Data and ADO Records Let Remote Users Execut
Microsoft Security Bulletin MS11-002 - Critical Microsoft Docs
MS11-002 (6451010)

ASA-2011-006 (2451910)
Microsoft Data Access Components ActiveX Data Objects Memory Corruption Vulnerability
CVE Program record
NVD vulnerability detail

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](#)