



CVE-2012-0182

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

Summary

CVE	CVE-2012-0182
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-10-09 21:55:00 UTC
Updated	2018-10-12 22:02:00 UTC
Description	Microsoft Word 2007 SP2 and SP3 does not properly handle memory during the parsing of Word documents, which allows

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Word	2007	sp2	All	All
Application	Microsoft	Word	2007	sp3	All	All
Application	Microsoft	Word	2007	sp2	All	All
Application	Microsoft	Word	2007	sp3	All	All

References

Reference	Source	Link	Tags
Microsoft Security Bulletin MS12-064 - Critical Microsoft Docs	MS	docs.microsoft.com	
Microsoft Word PAPX Section Corruption Remote Code Execution Vulnerability	BID	www.securityfocus.com	
Repository / Oval Repository	OVAL	oval.cisecurity.org	
US-CERT Alert TA12-283A - Microsoft Updates for Multiple Vulnerabilities	CERT	www.us-cert.gov	US Government Res
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#)