



CVE-2016-3281

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

Summary

CVE	CVE-2016-3281
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-07-13 01:59:00 UTC
Updated	2018-10-12 22:12:00 UTC
Description	Microsoft Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Office Web Apps	2010	sp2	All	All
Application	Microsoft	Office Web Apps	2010	sp2	All	All
Application	Microsoft	Sharepoint Server	2010	sp2	All	All
Application	Microsoft	Sharepoint Server	2010	sp2	All	All
Application	Microsoft	Word	2010	sp2	All	All
Application	Microsoft	Word	2013	sp1	All	All
Application	Microsoft	Word	2016	All	All	All
Application	Microsoft	Word	2010	sp2	All	All
Application	Microsoft	Word	2013	sp1	All	All
Application	Microsoft	Word	2016	All	All	All
Application	Microsoft	Word For Mac	2011	All	All	All
Application	Microsoft	Word For Mac	2016	All	All	All
Application	Microsoft	Word For Mac	2011	All	All	All
Application	Microsoft	Word For Mac	2016	All	All	All
Application	Microsoft	Word Rt	2013	sp1	All	All

Application	Microsoft	Word Rt	2013	sp1	All	All
-------------	-----------	---------	------	-----	-----	-----

References

Reference	Source
Microsoft SharePoint File Processing Flaws Lets Remote Users Obtain Potentially Sensitive Information - SecurityTracker	SECTRA
Microsoft Security Bulletin MS16-088 - Critical Microsoft Docs	MS
Microsoft Office CVE-2016-3281 Memory Corruption Vulnerability	BID
Microsoft Office Multiple File Processing Memory Corruption Errors Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRA
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.

© 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](#).

CVE.report and Source URL Uptime Status status.cve.report