



CVE-2015-2503

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

Summary

CVE	CVE-2015-2503
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-11-11 11:59:00 UTC
Updated	2018-10-12 22:09:00 UTC
Description	Microsoft Access 2007 SP3, Excel 2007 SP3, InfoPath 2007 SP3, OneNote 2007 SP3, PowerPoint 2007 SP3, Project 2007

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Access	2007	sp3	All	All
Application	Microsoft	Access	2010	sp2	All	All
Application	Microsoft	Access	2013	sp1	All	All
Application	Microsoft	Access	2016	All	All	All
Application	Microsoft	Access	2007	sp3	All	All
Application	Microsoft	Access	2010	sp2	All	All
Application	Microsoft	Access	2013	sp1	All	All
Application	Microsoft	Access	2016	All	All	All
Application	Microsoft	Excel	2007	sp3	All	All
Application	Microsoft	Excel	2010	sp2	All	All
Application	Microsoft	Excel	2010	sp2	All	All
Application	Microsoft	Excel	2013	sp1	All	All
Application	Microsoft	Excel	2013	sp1	All	All
Application	Microsoft	Excel	2016	All	All	All
Application	Microsoft	Excel	2007	sp3	All	All
Application	Microsoft	Excel	2010	sp2	All	All
Application	Microsoft	Excel	2010	sp2	All	All

Application	Microsoft	Excel	2013	sp1	All	All
Application	Microsoft	Excel	2013	sp1	All	All
Application	Microsoft	Excel	2016	All	All	All
Application	Microsoft	Infopath	2007	sp3	All	All
Application	Microsoft	Infopath	2010	sp2	All	All
Application	Microsoft	Infopath	2013	sp1	All	All
Application	Microsoft	Infopath	2007	sp3	All	All
Application	Microsoft	Infopath	2010	sp2	All	All
Application	Microsoft	Infopath	2013	sp1	All	All
Application	Microsoft	Lync	2013	sp1	All	All
Application	Microsoft	Lync	2013	sp1	All	All
Application	Microsoft	Office 2007 Ime	sp3	All	All	ja
Application	Microsoft	Office 2007 Ime	sp3	All	All	ja
Application	Microsoft	Onenote	2007	sp3	All	All
Application	Microsoft	Onenote	2010	sp2	All	All
Application	Microsoft	Onenote	2013	sp1	All	All
Application	Microsoft	Onenote	2013	sp1	All	All
Application	Microsoft	Onenote	2016	All	All	All
Application	Microsoft	Onenote	2007	sp3	All	All
Application	Microsoft	Onenote	2010	sp2	All	All
Application	Microsoft	Onenote	2013	sp1	All	All
Application	Microsoft	Onenote	2013	sp1	All	All
Application	Microsoft	Onenote	2016	All	All	All
Application	Microsoft	Pinyin Ime	2010	All	All	All
Application	Microsoft	Pinyin Ime	2010	All	All	All
Application	Microsoft	Powerpoint	2007	sp3	All	All
Application	Microsoft	Powerpoint	2010	sp2	All	All
Application	Microsoft	Powerpoint	2013	sp1	All	All
Application	Microsoft	Powerpoint	2013	sp1	All	All
Application	Microsoft	Powerpoint	2016	All	All	All
Application	Microsoft	Powerpoint	2007	sp3	All	All
Application	Microsoft	Powerpoint	2010	sp2	All	All
Application	Microsoft	Powerpoint	2013	sp1	All	All
Application	Microsoft	Powerpoint	2013	sp1	All	All
Application	Microsoft	Powerpoint	2016	All	All	All

Application	Microsoft	Project	2007	sp3	All	All
Application	Microsoft	Project	2016	All	All	All
Application	Microsoft	Project	2007	sp3	All	All
Application	Microsoft	Project	2016	All	All	All
Application	Microsoft	Project Server	2010	sp2	All	All
Application	Microsoft	Project Server	2013	sp1	All	All
Application	Microsoft	Project Server	2010	sp2	All	All
Application	Microsoft	Project Server	2013	sp1	All	All
Application	Microsoft	Publisher	2007	sp3	All	All
Application	Microsoft	Publisher	2010	sp2	All	All
Application	Microsoft	Publisher	2013	sp1	All	All
Application	Microsoft	Publisher	2016	All	All	All
Application	Microsoft	Publisher	2007	sp3	All	All
Application	Microsoft	Publisher	2010	sp2	All	All
Application	Microsoft	Publisher	2013	sp1	All	All
Application	Microsoft	Publisher	2016	All	All	All
Application	Microsoft	Skype For Business	2016	All	All	All
Application	Microsoft	Skype For Business	2016	All	All	All
Application	Microsoft	Visio	2007	sp3	All	All
Application	Microsoft	Visio	2010	sp2	All	All
Application	Microsoft	Visio	2013	sp1	All	All
Application	Microsoft	Visio	2016	All	All	All
Application	Microsoft	Visio	2007	sp3	All	All
Application	Microsoft	Visio	2010	sp2	All	All
Application	Microsoft	Visio	2013	sp1	All	All
Application	Microsoft	Visio	2016	All	All	All
Application	Microsoft	Word	2007	sp3	All	All
Application	Microsoft	Word	2010	sp2	All	All
Application	Microsoft	Word	2013	sp1	All	All
Application	Microsoft	Word	2013	sp1	All	All
Application	Microsoft	Word	2016	All	All	All
Application	Microsoft	Word	2007	sp3	All	All
Application	Microsoft	Word	2010	sp2	All	All
Application	Microsoft	Word	2013	sp1	All	All
Application	Microsoft	Word	2013	sp1	All	All

Application	Microsoft	Word	2016	All	All	All
References						
Reference						Source
Microsoft Security Bulletin MS15-116 - Important Microsoft Docs						MS
Microsoft Office Bugs Let Remote Users Bypass Sandbox Restrictions, Spoof Web Sites, and Execute Arbitrary Code - SecurityTracker						SE
Microsoft Lync Lets Remote Users Bypass Sandbox Restrictions on the Target System - SecurityTracker						SE
Microsoft Skype for Business Lets Remote Users Bypass Sandbox Restrictions on the Target System - SecurityTracker						SE
CVE Program record						CV
NVD vulnerability detail						NV
<div style="border: 1px solid #ccc; padding: 2px;"> ◀ ▶ </div>						
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