



CVE-2015-2423

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2015-2423
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-15 00:59:00 UTC
Updated	2019-05-15 11:53:00 UTC
Description	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Window

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Excel	2007	sp3	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	2007	sp3	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	Internet Explorer	10	All	All	All
Application	Microsoft	Internet Explorer	11	-	All	All
Application	Microsoft	Internet Explorer	7	All	All	All
Application	Microsoft	Internet Explorer	8	All	All	All
Application	Microsoft	Internet Explorer	9	All	All	All
Application	Microsoft	Internet Explorer	10	All	All	All
Application	Microsoft	Internet Explorer	11	-	All	All
Application	Microsoft	Internet Explorer	7	All	All	All
Application	Microsoft	Internet Explorer	8	All	All	All

Application	Microsoft	Internet Explorer	9	All	All	All
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Office	2010	sp2	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	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	Visio	2007	sp3	All	All
Application	Microsoft	Visio	2010	sp2	All	All
Application	Microsoft	Visio	2013	sp1	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	2013	sp1	All	All
Application	Microsoft	Visio	2016	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt	-	All	All	All
Operating System	Microsoft	Windows Rt	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All

Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Vista	-	sp2	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

Microsoft Security Bulletin MS15-079 - Critical | Microsoft Docs

Microsoft Internet Explorer Multiple Bugs Let Remote Users Bypass ASLR, Obtain Potentially Sensitive Information, and Execute Arbitrary Code - SecurityTracker

Microsoft Security Bulletin MS15-088 - Important | Microsoft Docs

Microsoft Security Bulletin MS15-081 - Critical | Microsoft Docs

Microsoft Windows Command Line Flaw Lets Remote Users Obtain Potentially Sensitive Information on the Target System - SecurityTracker

Microsoft Office Multiple Flaws Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information - SecurityTracker

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)