



CVE-2015-2379

Published on: 07/14/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:20 PM UTC

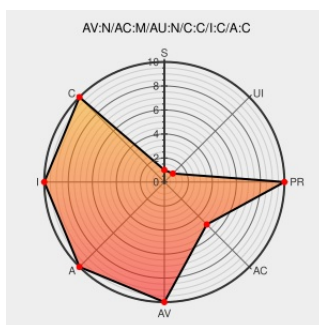
CVE-2015-2379

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Office](#) from [Microsoft](#) contain the following vulnerability:

Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Office for Mac 2011, and Word Viewer allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE-2015-2379 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

COMPLETE

Integrity Impact

COMPLETE

Availability Impact

COMPLETE

CVE References

Description

Tags

Link

Microsoft Security Bulletin MS15-070 - Important | Microsoft Docs

docs.microsoft.com
[text/html](#)

MS MS15-070

Microsoft Office Multiple Flaws Let Remote Users Bypass ASLR and Execute Arbitrary Code - SecurityTracker

www.securitytracker.com
[text/html](#)

SECTRAK 1032899

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Office	2011	All	All	All
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Office	2011	All	All	All
Application	Microsoft	Word	2007	sp3	All	All
Application	Microsoft	Word	2013	sp1	All	All
Application	Microsoft	Word	2013	sp1	All	All
Application	Microsoft	Word	2007	sp3	All	All
Application	Microsoft	Word	2013	sp1	All	All
Application	Microsoft	Word	2013	sp1	All	All
Application	Microsoft	Word Viewer	All	All	All	All
Application	Microsoft	Word Viewer	All	All	All	All
cpe:2.3:a:microsoft:office:2010:sp2:*:*:*:x64:*:						
cpe:2.3:a:microsoft:office:2010:sp2:*:*:*:x86:*:						
cpe:2.3:a:microsoft:office:2011:*:*:*:mac:*:*:						
cpe:2.3:a:microsoft:office:2010:sp2:*:*:*:x64:*:						
cpe:2.3:a:microsoft:office:2010:sp2:*:*:*:x86:*:						
cpe:2.3:a:microsoft:office:2011:*:*:*:mac:*:*:						
cpe:2.3:a:microsoft:word:2007:sp3:*:*:*:*:						
cpe:2.3:a:microsoft:word:2013:sp1:*:*:*:*:						
cpe:2.3:a:microsoft:word:2013:sp1:*:*:rt:*:*:						
cpe:2.3:a:microsoft:word:2007:sp3:*:*:*:*:						
cpe:2.3:a:microsoft:word:2013:sp1:*:*:*:*:						
cpe:2.3:a:microsoft:word:2013:sp1:*:*:rt:*:*:						
cpe:2.3:a:microsoft:word_viewer:*:*:*:*:*:						
cpe:2.3:a:microsoft:word_viewer:*:*:*:*:*:						

NO vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#)