



# CVE-2015-2424

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

## Summary

<b>CVE</b>	CVE-2015-2424
<b>State</b>	PUBLISHED
<b>Assigner</b>	microsoft
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-07-14 21:59:35 UTC
<b>Updated</b>	2026-04-22 16:30:45 UTC
<b>Description</b>	Microsoft PowerPoint 2007 SP3, Word 2007 SP3, PowerPoint 2010 SP2, Word 2010 SP2, PowerPoint 2013 SP1, Word 2013 SP1

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from ADP

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

**EPSS:** 0.644800000 probability, percentile 0.984620000 (date 2026-04-25)

**CISA KEV:** Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

**Problem Types:** CWE-787 | n/a | CWE-787 CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9.3		AV:N/AC:MAu:N/C:C/I:C/A:C

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

### CISA Known Exploited Vulnerability

<b>Vendor</b>	Microsoft
<b>Product</b>	PowerPoint
<b>Name</b>	Microsoft PowerPoint Memory Corruption Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2015-2424">https://nvd.nist.gov/vuln/detail/CVE-2015-2424</a>

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Excel Viewer	2007	sp3	All	All
Application	Microsoft	Office	2007	sp3	All	All
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Office	2011	All	All	All
Application	Microsoft	Office	2013	sp1	All	All
Application	Microsoft	Office	2013	sp1	All	All
Application	Microsoft	Office Compatibility Pack	-	sp3	All	All

Application	Microsoft	Powerpoint	2007	sp3	All	All
Application	Microsoft	Powerpoint	2010	sp2	All	All
Application	Microsoft	Word	2013	sp1	All	All
Application	Microsoft	Word Viewer	-	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

#### References

Reference	Source
Microsoft Office Multiple Flaws Let Remote Users Bypass ASLR and Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-5
Microsoft Security Bulletin MS15-070 - Important   Microsoft Docs	af854a3a-2127-422b-91ae-5
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

#### Additional Advisory Data

Source	Time	Event
ADP	2022-03-03T00:00:00.000Z	CVE-2015-2424 added to CISA KEV

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)