CVE-2014-4114

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-4114
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-15 10:55:07 UTC
Updated	2026-04-22 16:48:57 UTC
Description	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windov

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from ADP

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

EPSS: 0.920900000 probability, percentile 0.997160000 (date 2026-05-09)

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

Problem Types: NVD-CWE-noinfo | n/a | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/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:M/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/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

Vendor	Microsoft
Product	Windows
Name	Microsoft Windows Object Linking & Embedding (OLE) Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2014-4114

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 8	-	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 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 2012	-	gold	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All

Vendor Declared Affected Products

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

References

Reference	Source
osvdb.org/show/osvdb/113140	af854a3a-2127-422
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2
Microsoft Windows CVE-2014-4114 OLE Package Manager Remote Code Execution Vulnerability	af854a3a-2127-422
iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign - iSIGHT Partners	af854a3a-2127-422
Windows OLE - Remote Code Execution "Sandworm" Exploit (MS14-060)	af854a3a-2127-422
Microsoft Security Bulletin MS14-060 - Important | Microsoft Docs	af854a3a-2127-422
Windows OLE Package Manager SandWorm Exploit	af854a3a-2127-422
MS14-060 Microsoft Windows OLE Package Manager Code Execution	af854a3a-2127-422
Security Advisory SA60972 - Microsoft Windows OLE Object Handling Arbitrary Code Execution Vulnerability - Secunia	af854a3a-2127-422
An Analysis of Windows Zero-day Vulnerability ‘CVE-2014-4114’ aka "Sandworm"	af854a3a-2127-422
Assessing Risk for the October 2014 Security Updates - Security Research & Defense - Site Home - TechNet Blogs	af854a3a-2127-422
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-2014-4114 added to CISA KEV

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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

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