CVE-2014-6332

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

Summary

CVE	CVE-2014-6332
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-11 22:55:05 UTC
Updated	2026-04-22 16:46:45 UTC
Description	OleAut32.dll in OLE in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 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: 0.940940000 probability, percentile 0.999080000 (date 2026-04-25)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Unknown

Problem Types: CWE-119 | n/a | CWE-119 CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

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:M/Au: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

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

Vendor	Microsoft
Product	Windows
Name	Microsoft Windows Object Linking & Embedding (OLE) Automation Array Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2014-6332

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 2003	-	sp2	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 Vista	-	sp2	All	All

Vendor Declared Affected Products

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

References

Reference
forsec.nl/wp-content/uploads/2014/11/ms14_064_ie_olerce.rb_.txt
Microsoft Windows OLE Automation Array Remote Code Execution Vulnerability | US-CERT
Microsoft Windows CVE-2014-6332 OLE Remote Code Execution Vulnerability
Vulnerability Note VU#158647 - Microsoft Windows Object Linking and Embedding (OLE) OleAut32 library SafeArrayRedim function vulnerabl
Avant Browser Lite / Ultimate Remote Code Execution ≈ Packet Storm
Microsoft Windows HTA HTML Application - Remote Code Execution MS14-064 - Exploits Database
The World Browser 3.0 Final Remote Code Execution ≈ Packet Storm
Microsoft Compiled HTML Help Remote Code Execution ≈ Packet Storm
Microsoft Windows OLE Automation Array Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker
Microsoft Security Bulletin MS14-064 - Critical | Microsoft Docs
www.cisa.gov/known-exploited-vulnerabilities-catalog
HTML Compiler Remote Code Execution ≈ Packet Storm
The World Browser 3.0 Final - Remote Code Execution - Windows remote Exploit
HTML Compiler - Remote Code Execution - Windows remote Exploit
Winamp Bento Browser Remote Code Execution ≈ Packet Storm
Internet Download Manager - OLE Automation Array Remote Code Execution - Windows remote Exploit
IBM X-Force Researcher Finds Significant Vulnerability in Microsoft Windows
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-03-25T00:00:00.000Z	CVE-2014-6332 added to CISA KEV

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