



CVE-2014-4077

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

Summary

CVE	CVE-2014-4077
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-11 22:55:04 UTC
Updated	2026-04-22 13:54:19 UTC
Description	Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, and C

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

EPSS: 0.507950000 probability, percentile 0.978710000 (date 2026-04-22)

CISA KEV: Listed on 2022-05-25; due 2022-06-15; ransomware use Unknown

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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
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:MAu: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

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	Input Method Editor (IME) Japanese
Name	Microsoft IME Japanese Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2014-4077

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Office 2007 Ime	sp3	All	All	ja
Operating System	Microsoft	Windows 7	-	sp1	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 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
Microsoft Input Method Editor (Japanese) Sandbox Bypass Flaw Lets Remote Users Gain Elevated Privileges - SecurityTracker						af854a3a-2
Assessing Risk for the November 2014 Security Updates - Security Research & Defense - Site Home - TechNet Blogs						af854a3a-2
Microsoft Security Bulletin MS14-078 - Moderate Microsoft Docs						af854a3a-2
Microsoft Office IME Sandbox Bypass Flaw Lets Remote Users Gain Elevated Privileges - SecurityTracker						af854a3a-2
www.cisa.gov/known-exploited-vulnerabilities-catalog						134c704f-9
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	2022-05-25T00:00:00.000Z	CVE-2014-4077 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

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