



CVE-2015-0016

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

Summary

CVE	CVE-2015-0016
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-13 22:59:07 UTC
Updated	2026-04-22 16:46:33 UTC
Description	Directory traversal vulnerability in the TS WebProxy (aka TSWbPrxy) component in Microsoft Windows Vista SP2, Windows

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: 0.920940000 probability, percentile 0.997120000 (date 2026-04-21)

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

Problem Types: CWE-22 | n/a | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

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: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

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 TS WebProxy Directory Traversal Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2015-0016

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	-	gold	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	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
MS15-004 Microsoft Remote Desktop Services Web Proxy IE Sandbox Escape ~ Packet Storm	af854a
Security Advisory SA62076 - Microsoft Windows TS WebProxy Windows Component Security Bypass Vulnerability - Secunia	af854a
CVE-2015-0016: Escaping the Internet Explorer Sandbox	af854a
MS15-004 Microsoft Remote Desktop Services Web Proxy IE Sandbox Escape	af854a
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c70
Microsoft Windows CVE-2015-0016 Remote Privilege Escalation Vulnerability	af854a
Microsoft Windows TS WebProxy Component Directory Traversal Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker	af854a
Microsoft Security Bulletin MS15-004 - Important Microsoft Docs	af854a
CruiseWorks and Minna De Office Access Restrictions Bypass Vulnerability	af854a
IBM X-Force Exchange	af854a
CVE Program record	CVE.O
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-2015-0016 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 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