CVE-2010-2568

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

Summary

CVE	CVE-2010-2568
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-07-22 05:43:49 UTC
Updated	2026-04-22 10:35:13 UTC
Description	Windows Shell in Microsoft Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 SP2 and R2, and Windo

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: 0.921340000 probability, percentile 0.997140000 (date 2026-04-21)

CISA KEV: Listed on 2022-09-15; due 2022-10-06; 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 Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-046; https://nvd.nist.gov/vuln/detail/CVE-2010-2568

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 7	-	All	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	-	-	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	All	All	All
Operating System	Microsoft	Windows Server 2008	r2	All	All	All
Operating System	Microsoft	Windows Vista		sp1	All	All

Operating System	Microsoft	Windows Vista	-	sp1	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp3	All	All

Vendor Declared Affected Products

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

References

Reference	Source
US-CERT Vulnerability Note VU#940193	af854a3a-2127
US-CERT Technical Cyber Security Alert TA10-222A -- Microsoft Updates for Multiple Vulnerabilities	af854a3a-2127
About Secunia Research | Flexera	af854a3a-2127
Espionage Attack Uses LNK Shortcut Files - F-Secure Weblog : News from the Lab	af854a3a-2127
Vulnerability in Windows "LNK" files?	af854a3a-2127
Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability	af854a3a-2127
Experts Warn of New Windows Shortcut Flaw — Krebs on Security	af854a3a-2127
Your request has been blocked. This could be due to several reasons.	af854a3a-2127
www.f-secure.com/weblog/archives/new_rootkit_en.pdf	af854a3a-2127
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21
SecurityTracker.com Archives - Microsoft Windows Shell LNK Shortcut Processing Flaw Lets Users Execute Arbitrary Code	af854a3a-2127
The CPL Icon Loading Vulnerability	af854a3a-2127
Repository / Oval Repository	af854a3a-2127
Microsoft Security Bulletin MS10-046 - Critical | Microsoft Docs	af854a3a-2127
Preempting a Major Issue Due to the LNK Vulnerability - Raising Infocon to Yellow	af854a3a-2127
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	2022-09-15T00:00:00.000Z	CVE-2010-2568 added to CISA KEV

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

Free CVE JSON API cve.report/api

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