



CVE-2009-1123

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

Summary

CVE	CVE-2009-1123
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-06-10 18:30:00 UTC
Updated	2026-04-22 13:52:26 UTC
Description	The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 20

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: 0.051710000 probability, percentile 0.899400000 (date 2026-05-02)

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	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	7.2		AV:L/AC:L/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

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Windows
Name	Microsoft Windows Improper Input Validation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2009-1123

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2000	-	sp4	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	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	-	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 Technical Cyber Security Alert TA09-160A -- Microsoft Updates for Multiple Vulnerabilities					af854a3a-2127	
Microsoft Security Bulletin MS09-025 - Important Microsoft Docs					af854a3a-2127	
www.cisa.gov/known-exploited-vulnerabilities-catalog					134c704f-9b21	
Repository / Oval Repository					af854a3a-2127	
osvdb.org/54940					af854a3a-2127	
SecurityTracker.com Archives - Windows Kernel Bugs Let Local Users Gain Elevated Privileges					af854a3a-2127	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH					af854a3a-2127	
Microsoft Windows Kernel Privilege Escalation Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com					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	2022-03-03T00:00:00.000Z		CVE-2009-1123 added to CISA KEV			
There are currently no legacy QID mappings associated with this CVE.						