CVE-2013-5065

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

Summary

CVE	CVE-2013-5065
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-11-28 00:55:04 UTC
Updated	2026-04-22 16:45:57 UTC
Description	NDProxy.sys in the kernel in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privilege

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: 0.735800000 probability, percentile 0.988200000 (date 2026-04-28)

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 Kernel Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2013-5065

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2003 Server	-	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
Windows NDProxy - Privilege Escalation XP SP3 x86 and 2003 SP2 x86 MS14-002 - Exploits Database	af854a3a-2127-422b-9
Microsoft Security Advisory (2914486): Vulnerability in Microsoft Windows Kernel Could Allow Elevation of Privilege	af854a3a-2127-422b-9
MS Windows Local Privilege Escalation Zero-Day in The Wild | FireEye Blog	af854a3a-2127-422b-9
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91
Microsoft Security Bulletin MS14-002 - Important | Microsoft Docs	af854a3a-2127-422b-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	2022-03-03T00:00:00.000Z	CVE-2013-5065 added to CISA KEV

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