CVE-2013-3660

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

Summary

CVE	CVE-2013-3660
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-05-24 20:55:01 UTC
Updated	2026-04-22 13:43:34 UTC
Description	The EPATHOBJ::pprFlattenRec function in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, V

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: 0.706320000 probability, percentile 0.987080000 (date 2026-05-01)

CISA KEV: Listed on 2022-03-28; due 2022-04-18; ransomware use Unknown

Problem Types: CWE-119 | n/a | CWE-119 CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

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	6.9		AV:L/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

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Win32k
Name	Microsoft Win32k Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2013-3660

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 Rt	-	All	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 2012	-	All	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
Google engineer publicizes Windows zero-day bug, claims Microsoft is 'difficult to work with' | The Verge
win32k!EPATHOBJ::pprFlattenRec Uninitialized Next Pointer Testcase
NEOHAPSIS - Peace of Mind Through Integrity and Insight
0day: Windows Kernel EPATHOBJ Vulnerability : netsec
www.cisa.gov/known-exploited-vulnerabilities-catalog
Tavis Ormandy na Twitterze: "I just realised a really cute trick to exploit the EPATHOBJ bug, make the list cycle, then a thread can clean up th
Tavis Ormandy na Twitterze: "Testing win32k under memory pressure, this causes an EPATHOBJ to end up in userspace. Anyone want to inv
www.osvdb.org/93539
NEOHAPSIS - Peace of Mind Through Integrity and Insight
Google engineer bashes Microsoft's handling of security researchers, discloses Windows zero-day | Computerworld
Repository / Oval Repository
Security Advisory SA53435 - Microsoft Windows Kernel Multiple Vulnerabilities - Secunia
NEOHAPSIS - Peace of Mind Through Integrity and Insight
Microsoft Updates for Multiple Vulnerabilities | US-CERT
Microsoft Security Bulletin MS13-053 - Critical | Microsoft Docs
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-03-28T00:00:00.000Z	CVE-2013-3660 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