



CVE-2010-4398

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

Summary

CVE	CVE-2010-4398
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-12-06 13:44:54 UTC
Updated	2026-04-21 20:30:28 UTC
Description	Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys in Microsoft Windows XP SP2 and SP3, '...

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.079360000 probability, percentile 0.920960000 (date 2026-05-11)

CISA KEV: Listed on 2022-03-28; due 2022-04-21; ransomware use Unknown

Problem Types: CWE-787 | n/a | CWE-787 CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/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:L/UI:N/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

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/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 Stack-Based Buffer Overflow Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2010-4398

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	All
Operating System	Microsoft	Windows Server 2008	-	sp2	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	-	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
Repository / Oval Repository	af854a3a-21
ASA-2011-031 (2393802)	af854a3a-21
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b
Microsoft Windows win32k.sys Driver "GreEnableEUDC()" Vulnerability - Advisories - Community	af854a3a-21
Elevation of privileges under Windows Vista/7 (UAC Bypass) 0day	af854a3a-21
Bypassing UAC with User Privilege under Windows Vista/7 – Mirror	af854a3a-21
US-CERT Vulnerability Note VU#529673	af854a3a-21
New Windows zero-day flaw bypasses UAC Naked Security	af854a3a-21
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-21
Privilege escalation 0-day in almost all Windows versions	af854a3a-21
Microsoft Security Bulletin MS11-011 - Important Microsoft Docs	af854a3a-21
Microsoft Windows User Access Control (UAC) Bypass Local Privilege Escalation Vulnerability	af854a3a-21
Security Response on Twitter: "We 're investigating public PoC for a local EoP vuln requiring an account on the target system"	af854a3a-21
Windows Kernel Lets Local Users Gain Elevated Privileges - SecurityTracker	af854a3a-21
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	2022-03-28T00:00:00.000Z	CVE-2010-4398 added to CISA KEV

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#)