



CVE-2015-1701

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

Summary

CVE	CVE-2015-1701
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-21 10:59:00 UTC
Updated	2020-05-14 21:15:00 UTC
Description	Win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Vista SP2, and Server 2008 SP2 allows loc

Risk And Classification

EPSS: 0.902620000 probability, percentile 0.995930000 (date 2026-04-01)

CISA KEV: Listed on 2022-03-03; due 2022-03-24; ransomware use Known

Problem Types: CWE-264

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-2015-1701

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

Full Disclosure: KL-001-2020-002 : Cellebrite Restricted Desktop Escape and Escalation of User Privilege

Microsoft Security Bulletin MS15-051 - Important | Microsoft Docs

Microsoft Windows Unspecified Flaw Lets Local Users Gain System Privileges - SecurityTracker

Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack « Threat Research

Microsoft Windows - ClientCopyImage Win32k (MS15-051) (Metasploit) - Windows local Exploit

Microsoft Windows - Local Privilege Escalation (MS15-051) - Windows local Exploit

Symantec na Twitterze: "TRENDING: RussianDoll #APT28 campaign found using Flash vuln + Windows #0Day. Update #AdobeFlash to stay

Microsoft Windows CVE-2015-1701 Local Privilege Escalation Vulnerability

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog



No vendor comments have been submitted for this CVE.

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)