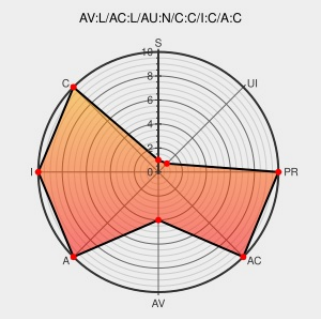
CVE-2010-2739

Published on: 09/07/2010 12:00:00 AM UTC

Last Modified on: 07/07/2021 04:09:00 PM UTC

CVE-2010-2739

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows 2003 Server from Microsoft contain the following vulnerability:

Buffer overflow in the CreateDIBPalette function in win32k.sys in Microsoft Windows XP SP3, Server 2003 R2 Enterprise SP2, Vista Business SP1, Windows 7, and Server 2008 SP2 allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.

CVE-2010-2739 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory, www.vupen.com, text/html	VUPEN ADV-2010-2029
Microsoft Windows win32k.sys Driver "CreateDIBPalette()" Buffer Overflow - Advisories - Community	Vendor Advisory, web.archive.org, text/html	SECUNIA 40870
Heapos Forever « Insanely Low-Level	Exploit, www.ragestorm.net, text/html	MISC www.ragestorm.net/blogs/?p=255
Update on the publicly disclosed Win32k.sys EoP Vulnerability - The Microsoft Security Response Center (MSRC) - Site	Vendor Advisory, blogs.technet.com	CONFIRM blogs.technet.com/b/msrc/archive/2010/08/10/update-

The Microsoft Security Response Center (MSRC) Site Home - TechNet Blogs	text/html	blogs.technet.com/b/msrc/archive/2014/06/13/update-on-the-publicly-disclosed-win32k-sys-eop-vulnerability.aspx

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2003 Server	All	r2	All	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	enterprise	All
Operating System	Microsoft	Windows 2003 Server	All	r2	All	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	enterprise	All
Operating System	Microsoft	Windows 7	All	All	All	All
Operating System	Microsoft	Windows 7	All	All	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	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	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All

cpe:2.3:o:microsoft:windows_2003_server:*:r2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:*:sp2:enterprise:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:*:r2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:*:sp2:enterprise:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_7:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_7:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→