

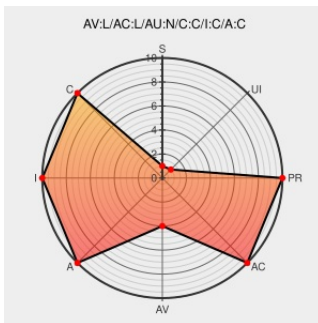


CVE-2010-2739

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

LOCAL

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

COMPLETE

Integrity Impact

COMPLETE

Availability Impact

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-

There are currently no QIDs associated with this CVE

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→

© CVE.report 2023 |

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