



CVE-2005-0416

Published on: 02/14/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:25 PM UTC

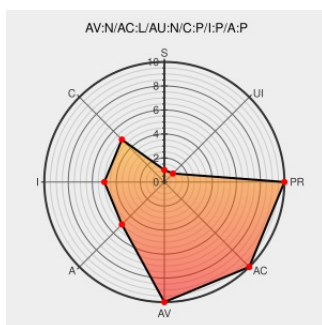
CVE-2005-0416

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Windows 2000](#) from [Microsoft](#) contain the following vulnerability:

The Windows Animated Cursor (ANI) capability in Windows NT, Windows 2000 through SP4, Windows XP through SP1, and Windows 2003 allows remote attackers to execute arbitrary code via the AnimationHeaderBlock length field, which leads to a stack-based buffer overflow.

CVE-2005-0416 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

PARTIAL

CVE References

Description

Tags

Link

Network Security, Vulnerability Assessment, Intrusion Prevention

[eeye.com](#)
[text/html](#)

[MISC](#)
eeye.com/html/research/advisories/AD20050111.html

Microsoft Windows User32.DLL ANI File Header Handling Stack-Based Buffer Overflow Vulnerability

[Exploit](#)
[Patch](#)
[Vendor Advisory](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 12233](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF win-user32-aniheader-overflow\(18879\)](#)

Microsoft Security Bulletin MS05-002 - Critical | Microsoft Docs

[docs.microsoft.com](#)
[text/html](#)

[MS MS05-002](#)

'Windows ANI File Parsing Proof Of Concept (MS05-002)' - MARC		marc.info text/html	 BUGTRAQ 20050112 Windows ANI File Parsing Proof Of Concept (MS05-002)			
'EEYE: Windows ANI File Parsing Buffer Overflow' - MARC		marc.info text/html	 BUGTRAQ 20050111 EEYE: Windows ANI File Parsing Buffer Overflow			
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.						
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 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	r2	All	datacenter_64-bit	All
Operating System	Microsoft	Windows 2003 Server	standard	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All

Operating System	Microsoft	Windows 2003 Server	enterprise	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	r2	All	datacenter_64-bit	All
Operating System	Microsoft	Windows 2003 Server	standard	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows 98	All	gold	All	All
Operating System	Microsoft	Windows 98	All	gold	All	All
Operating System	Microsoft	Windows 98se	All	All	All	All
Operating System	Microsoft	Windows 98se	All	All	All	All
Operating System	Microsoft	Windows Me	All	All	All	All
Operating System	Microsoft	Windows Me	All	All	All	All
Operating System	Microsoft	Windows Nt	4.0	All	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	All	server	All
Operating System	Microsoft	Windows Nt	4.0	All	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	All	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp1	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp2	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	terminal_server	All

Operating System	Microsoft	Windows Nt	4.0	sp2	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp3	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp4	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp5	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	workstation	All
Operating System	Microsoft	Windows Nt	4.0	All	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	All	server	All
Operating System	Microsoft	Windows Nt	4.0	All	terminal_server	All

Operating System	Microsoft	Windows Nt	4.0	All	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp1	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp2	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp3	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp4	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp5	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	server	All

Operating System	Microsoft	Windows Nt	4.0	sp6	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	workstation	All
Operating System	Microsoft	Windows Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	All	embedded	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	All	media_center	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	64-bit	All
Operating System	Microsoft	Windows Xp	All	sp1	embedded	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	All	embedded	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	All	media_center	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	64-bit	All
Operating System	Microsoft	Windows Xp	All	sp1	embedded	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All

Operating System	Microsoft	Windows Xp	All	sp1	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All
cpe:2.3:o:microsoft:windows_2000:*:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2000*:sp1:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2000*:sp2:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2000*:sp3:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2000*:sp4:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2000:*:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2000*:sp1:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2000*:sp2:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2000*:sp3:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2000*:sp4:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:enterprise*:64-bit:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:enterprise_64-bit:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:r2*:64-bit:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:r2*:datacenter_64-bit:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:standard*:64-bit:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:web:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:enterprise*:64-bit:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:enterprise_64-bit:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:r2*:64-bit:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:r2*:datacenter_64-bit:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:standard*:64-bit:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:web:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_98*:gold:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_98*:gold:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_98se:*:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_98se:*:*:*:*:*:*:						

```
cpe:2.3:o:microsoft:windows_me:*.:.:.:.:.:.:.:
```

```
cpe:2.3:o:microsoft:windows_me:*.:.:.:.:.:.:.:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:*:enterprise_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:*:server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:*:terminal_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0*:workstation:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp1:enterprise_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows nt:4.0:sp1:server:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows nt:4.0:sp1:terminal server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp1:workstation:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp2:enterprise_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp2:server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows nt:4.0:sp2:terminal server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp2:workstation:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:enterprise_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:terminal_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:workstation:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows nt:4.0:sp4:enterprise server:*:*:*.*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp4:server:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp4:terminal_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp4:workstation:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows nt:4.0:sp5:enterprise server:*:*:*.*.*
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp5:server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows nt:4.0:sp5:terminal server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp5:workstation:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp6:enterprise_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp6:server:*:*:*:*:
```



```
cpe:2.3:o:microsoft:windows_nt:4.0:sp6:terminal_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp6:workstation:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows nt:4.0:sp6a:enterprise server:*:*:*.*
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows nt:4.0:sp6a:workstation:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0*:enterprise_server*::*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0*:server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows nt:4.0:*:terminal server:*:*:*.*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:*:workstation:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp1:enterprise_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp1:server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows nt:4.0:sp1:terminal server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp1:workstation:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp2:enterprise_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp2:server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp2:terminal_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp2:workstation:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:enterprise_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:terminal_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:workstation:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp4:enterprise_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp4:server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp4:terminal_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp4:workstation:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp5:enterprise_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp5:server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows nt:4.0:sp5:terminal server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp5:workstation:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows nt:4.0:sp6:enterprise server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp6:server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp6:terminal_server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp6:workstation:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:enterprise_server:*:*:*.*.*
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:server:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:workstation:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_xp:*:*:64-bit:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows xp:*:*:embedded:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows xp:*:*:home:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:*:media_center:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:gold:professional:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:sp1:64-bit:*:*:*:*:
```

cpe:2.3:o:microsoft:windows_xp:*:sp1:embedded:*:*:*:*:

```
cpe:2.3:o:microsoft:windows_xp:*.sp1:home:*.:.:.:.:
```

```
cpe:2.3:o:microsoft:windows_xp:*:sp1:media_center:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:sp2:tablet_pc:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_xp:*:*:64-bit:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:*:embedded:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:*:home:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_xp:*:*:media_center:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:gold:professional:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:sp1:64-bit:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows xp:*:sp1:embedded:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_xp:*.sp1:home:*.:.:.:.:
```

```
cpe:2.3:o:microsoft:windows_xp*:sp1:media_center:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:sp2:tablet_pc:*:*:*:*:*
```

[← 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](#)