

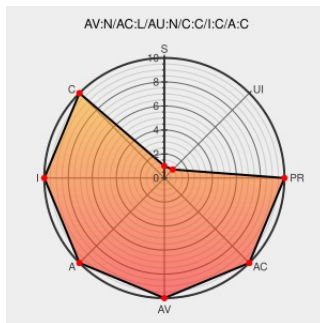


CVE-2005-1208

Published on: 06/14/2005 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1208

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Integer overflow in Microsoft Windows 98, 2000, XP SP2 and earlier, and Server 2003 SP1 and earlier allows remote attackers to execute arbitrary code via a crafted compiled Help (.CHM) file with a large size field that triggers a heap-based buffer overflow, as demonstrated using a "ms-its:" URL in Internet Explorer.

CVE-2005-1208 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

US-CERT Vulnerability Note VU#851869

Tags

[Patch](#)
[Third Party Advisory](#)
[US Government Resource](#)
www.kb.cert.org
[text/html](#)

Link

[CERT-VN VU#851869](#)

Repository / Oval Repository

oval.cisecurity.org
[text/html](#)

[OVAL oval.org.mitre.oval:def:381](#)

Repository / Oval Repository

oval.cisecurity.org
[text/html](#)

[OVAL oval.org.mitre.oval:def:463](#)

Repository / Oval Repository

oval.cisecurity.org
[text/html](#)

[OVAL oval.org.mitre.oval:def:1057](#)

Secunia - Advisories - Microsoft Windows HTML Help Input Validation Vulnerability	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 15683
US-CERT Technical Cyber Security Alert TA05-165A -- Microsoft Windows and Internet Explorer Vulnerabilities	Patch Third Party Advisory US Government Resource www.us-cert.gov text/html	 CERT TA05-165A
Neohapsis Archives - VulnWatch - #0062 - [VulnWatch] eEye Advisory - EEYEB-20050316 - HTML Help File Parsing Buffer Overflow	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 VULNWATCH 20050614 eEye Advisory - EEYEB-20050316 - HTML Help File Parsing Buffer Overflow
Microsoft Windows HTML Help Remote Code Execution Vulnerability	cve.report (archive) text/html	 BID 13953
Microsoft Security Bulletin MS05-026 - Critical Microsoft Docs	docs.microsoft.com text/html	 MS MS05-026

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	All	All	All
Operating System	Microsoft	Windows 2003 Server	64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_64-bit	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	enterprise	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	sp1_beta_1	All	All

Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	r2	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	r2	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	r2	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	standard	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	standard	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	standard	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	standard_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_64-bit	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	enterprise	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	64-bit	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	r2	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	r2	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	standard	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	standard	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	standard	sp1_beta_1	All	All
Operating System	Microsoft	Windows 2003 Server	standard_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1_beta_1	All	All
Operating System	Microsoft	Windows 98	All	gold	All	All
Operating System	Microsoft	Windows 98	All	gold	All	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	All	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	sp1	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	sp2	home	All
Operating System	Microsoft	Windows Xp	All	sp2	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	All	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	sp1	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	sp2	home	All
Operating System	Microsoft	Windows Xp	All	sp2	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:*:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:64-bit:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:datacenter_64-bit:sp1:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:datacenter_64-bit:sp1_beta_1:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server:enterprise:*:64-bit:*:*:*:*:						

cpe:2.3:o:microsoft:windows_2003_server:enterprise:sp1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:enterprise:sp1_beta_1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:enterprise_64-bit:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:enterprise_64-bit:sp1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:enterprise_64-bit:sp1_beta_1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:r2:*:*:*:*:*:
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:r2:sp1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:r2:sp1_beta_1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:standard:*:64-bit:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:standard:sp1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:standard:sp1_beta_1:*:*:*:*:*:
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:web:sp1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:web:sp1_beta_1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:64-bit:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:datacenter_64-bit:sp1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:datacenter_64-bit:sp1_beta_1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:enterprise:*:64-bit:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:enterprise:sp1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:enterprise:sp1_beta_1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:enterprise_64-bit:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:enterprise_64-bit:sp1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:enterprise_64-bit:sp1_beta_1:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2003_server:r2:*:*:*:*:*:
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:r2:sp1:*.:.:.:.:
```

```
cpe:2.3:o:microsoft:windows_2003_server:r2:sp1_beta_1:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_2003_server:standard:*:64-bit:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_2003_server:standard:sp1:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:o:microsoft:windows_2003_server:standard:sp1_beta_1:::*.*.*.*.*
```

```
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:web:sp1:.*:.*:.*:.*:.*:.*
```

cpe:2.3:o:microsoft:windows_2003_server:web:sp1_beta_1:*:*:*:*.*

```
cpe:2.3:o:microsoft:windows_98:*:gold:*.:.:.:.:
```

cpe:2.3:o:microsoft:windows_98:*:gold:*:*:*:*:*

```
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:*:*:*:*:*:
```

```
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:*:sp1:tablet_pc:*:*:*:*:
```

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

cpe:2.3:o:microsoft:windows_xp:*:sp2: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:*:*:*:*:
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:*:*:sp1:tablet_pc:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:*:sp2:home:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:*:sp2:media_center:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:*:sp2:tablet_pc:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)