

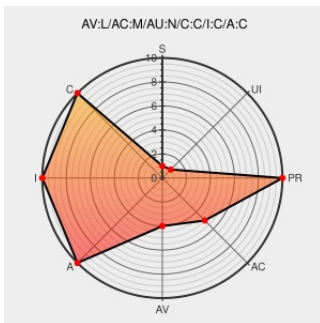


CVE-2009-2516

Published on: 10/14/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:31 PM UTC

CVE-2009-2516

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

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

The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold and SP1, and Server 2008 Gold does not properly validate data sent from user mode, which allows local users to gain privileges via a crafted PE .exe file that triggers a NULL pointer dereference during chain traversal, aka "Windows Kernel NULL Pointer Dereference Vulnerability."

CVE-2009-2516 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: **6.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
NSFOCUS - Windows Kernel Malformed PE File Remote DoS Vulnerability(SA2009-03)	web.archive.org text/html Inactive Link Not Archived	MISC www.nsfocus.com/en/advisories/0903.html
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval.org/mitre/oval:def:6264
US-CERT Technical Cyber Security Alert TA09-286A -- Microsoft Updates for Multiple Vulnerabilities	US Government Resource www.us-cert.gov text/xml	CERT TA09-286A
Microsoft Security Bulletin MS09-058 - Important Microsoft Docs	docs.microsoft.com text/html	MS MS09-058

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	sp4	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	x32	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	x32	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Vista	All	All	All	All
Operating System	Microsoft	Windows Vista	All	All	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	All	All	All
Operating System	Microsoft	Windows Vista	All	All	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All


```
cpe:2.3:0:microsoft:windows_vista::sp1:x64:::..:..:
```

```
cpe:2.3:o:microsoft:windows_vista:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_vista:*:*:x64:*:*:*:*:
```

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

```
cpe:2.3:o:microsoft:windows_vista:*:sp1:x64:*:*:*:*:
```

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

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

```
cpe:2.3:o:microsoft:windows_xp:*:sp2:professional_x64:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:sp2:x64:*:*:*:*:
```

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

```
cpe:2.3:o:microsoft:windows_xp:*:x64:*:*:*:*:*:
```

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

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

```
cpe:2.3:o:microsoft:windows_xp:*:sp2:professional_x64:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:sp2:x64:*:*:*:*:
```

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

```
cpe:2.3:o:microsoft:windows_xp:*:x64:*:*:*:*:*:*
```

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