

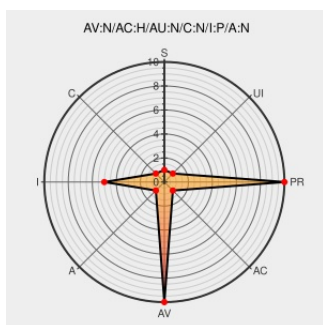


CVE-2005-2126

Published on: 10/21/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2126

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

Certain versions of **le** from **Microsoft** contain the following vulnerability:

The FTP client in Windows XP SP1 and Server 2003, and Internet Explorer 6 SP1 on Windows 2000 SP4, when "Enable Folder View for FTP Sites" is enabled and the user manually initiates a file transfer, allows user-assisted, remote FTP servers to overwrite files in arbitrary locations via crafted filenames.

CVE-2005-2126 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: **2.6 - LOW**

Access Vector

NETWORK

Access Complexity

HIGH

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Tags

Link

Repository / Oval Repository

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

[OVAL oval:org.mitre.oval:def:1284](#)

Repository / Oval Repository

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

[OVAL oval:org.mitre.oval:def:1146](#)

Microsoft Security Bulletin MS05-044 - Moderate | Microsoft Docs

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

[MS MS05-044](#)

Repository / Oval Repository

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

[OVAL oval:org.mitre.oval:def:1416](#)

Secunia - Advisories - Avaya Various Products Multiple Vulnerabilities

[web.archive.org](#)
[text/html](#)

[SECUNIA 17172](#)

US-CERT Vulnerability Note VU#415828

[Third Party Advisory](#)
[US Government Resource](#)

[CERT-VN VU#415828](#)

	www.kb.cert.org text/html	
SecuriTeam.com TM - Windows FTP Client Allows File Transfer Location Tampering (MS05-044)	Patch www.securiteam.com text/html	 MISC www.securiteam.com/windowsntfocus/6M00I0KEAU.html
	support.avaya.com application/pdf	 CONFIRM support.avaya.com/elmodocs2/security/ASA-2005-214.pdf
Secunia - Advisories - Microsoft Windows FTP Client Filename Validation Vulnerability	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 17163
SecurityTracker.com Archives - Microsoft Windows FTP Client Input Validation Hole Lets Remote Servers Create/Overwrite Files on the Target User's System	securitytracker.com text/html	 SECTrack 1015036
Secunia - Advisories - Nortel Centrex IP Client Manager Multiple Vulnerabilities	web.archive.org text/html	 SECUNIA 17223

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
Application	Microsoft	ie	6.0	sp1	All	All
Application	Microsoft	ie	6.0	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	fr
Operating System	Microsoft	Windows 2000	All	sp4	All	fr
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows Xp	All	sp1	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	sp1	tablet_pc	All
cpe:2.3:a:microsoft:ie:6.0:sp1:*****::						
cpe:2.3:a:microsoft:ie:6.0:sp1:*****::						
cpe:2.3:o:microsoft:windows_2000:*:sp4:*:fr:*****::						
cpe:2.3:o:microsoft:windows_2000:*:sp4:*:fr:*****::						

cpe:2.3:o:microsoft:windows_2003_server:r2:*:*:*:*:*:	
cpe:2.3:o:microsoft:windows_2003_server:r2:*:*:*:*:*:	
cpe:2.3:o:microsoft:windows_xp:*:sp1:tablet_pc:*:*:*:*:	
cpe:2.3:o:microsoft:windows_xp:*:sp1:tablet_pc:*:*:*:*:	
No vendor comments have been submitted for this CVE	
← Previous ID	Next ID→