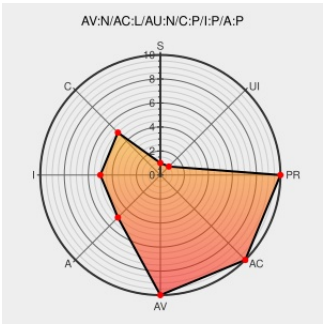
CVE-2005-4560

Published on: 12/28/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:20 PM UTC

CVE-2005-4560

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows 2003 Server from Microsoft contain the following vulnerability:

The Windows Graphical Device Interface library (GDI32.DLL) in Microsoft Windows allows remote attackers to execute arbitrary code via a Windows Metafile (WMF) format image with a crafted SETABORTPROC GDI Escape function call, related to the Windows Picture and Fax Viewer (SHIMGVW.DLL), a different vulnerability than CVE-2005-2123 and CVE-2005-2124, and as originally discovered in the wild on unionseek.com.

CVE-2005-4560 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Secunia - Advisories - Microsoft Windows WMF "SETABORTPROC" Arbitrary Code Execution	Vendor Advisory, web.archive.org, text/html	SECUNIA 18255
SecurityFocus	www.securityfocus.com, text/html	BUGTRAQ 20051229 WMF exploit
US-CERT Technical Cyber Security Alert TA05-362A -- Microsoft Windows Metafile Handling Buffer Overflow	Third Party Advisory, US Government Resource, www.us-cert.gov, text/html	CERT TA05-362A

Secunia - Advisories - Avaya Products Microsoft Windows WMF "SETABORTPROC" Vulnerability	Vendor Advisory web.archive.org text/html	SECUNIA 18364
Microsoft Security Advisory (912840): Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution.	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.microsoft.com/technet/security/advisory/912840.mspx
Secunia - Advisories - Nortel Products Microsoft Windows WMF "SETABORTPROC" Code Execution	Vendor Advisory web.archive.org text/html	SECUNIA 18415
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060103 WMF SETABORTPROC exploit
US-CERT Vulnerability Note VU#181038	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#181038
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051228 Re: Is this a new exploit?
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051228 WMF Exploit
News from the Lab Archive : January 2004 to September 2015	Exploit Vendor Advisory www.f-secure.com text/html	MISC www.f-secure.com/weblog/archives/archive-122005.html#00000753
	www130.nortelnetworks.com text/plain Inactive Link Not Archived	MISC www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=BLTNDETAIL&DocumentOID=375341
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060103 Re: [funsec] WMF round-up, updates and de-mystification
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060101 Re: RE: WMF Exploit
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2005-3086
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051227 Is this a new exploit?
Nortel Centrex IP Client Manager Multiple Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 18311
No Description Provided	Vendor Advisory support.avaya.com text/html	MISC support.avaya.com/elmodocs2/security/ASA-2006-001.htm
US-CERT Technical Cyber Security Alert TA06-005A -- Update for Microsoft Windows Metafile Vulnerability	Third Party Advisory US Government Resource www.us-cert.gov text/html	CERT TA06-005A
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF win-wmf-execute-code(23846)
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1460

SecurityTracker.com Archives - Microsoft Windows Unspecified WMF Rendering Bug Lets Remote Users Execute Arbitrary Code	Exploit securitytracker.com text/html	SECTRACK 1015416
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1431
Exploit-WMF	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC vil.mcafeesecurity.com/vil/content/v_137760.htm
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1433
Nortel: Technical Support	web.archive.org text/html Inactive Link Not Archived	MISC www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=BLTNDETAIL&DocumentOID=375420
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060104 Another WMF exploit workaround
Microsoft Windows Graphics Rendering Engine WMF SetAbortProc Code Execution Vulnerability	Exploit cve.report (archive) text/html	BID 16074
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051229 RE: WMF Exploit
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1612
[funsec] WMF Exploits overview draft	web.archive.org text/html Inactive Link Not Archived	MISC linuxbox.org/pipermail/funsec/2006-January/002455.html
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1492
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051227 Exploitation of Windows WMF on the web
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1564
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051228 RE: [Full-disclosure] Someone wasted a nice bug on spyware...
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060103 WMF round-up, updates and de-mystification
Microsoft Security Bulletin MS06-001 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS06-001

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 2003 Server	enterprise	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	enterprise	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	r2	sp1	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	web	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1	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	r2	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	r2	sp1	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	web	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1	All	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	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	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	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	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	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_2003_server:enterprise:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:enterprise:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:r2:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:r2:sp1:*:*:*:*:*:*:

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:web:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:web:sp1:*:*:*:*:*:*:

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:r2:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:r2:sp1:*:*:*:*:*:*:

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:web:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:web:sp1:*:*:*:*:*:*:

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:home:*:*:*:*:*:

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

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:*:*: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:home:*:*:*:*:*:

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

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→