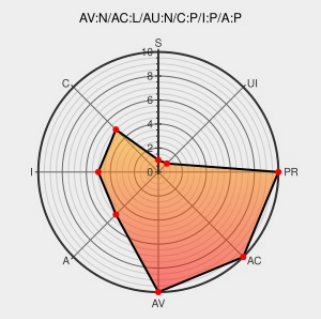
CVE-2005-2123

Published on: 11/29/2005 12:00:00 AM UTC

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

CVE-2005-2123

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



Certain versions of Windows 2000 from Microsoft contain the following vulnerability:

Multiple integer overflows in the Graphics Rendering Engine (GDI32.DLL) in Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 allow remote attackers to execute arbitrary code via crafted Windows Metafile (WMF) and Enhanced Metafile (EMF) format images that lead to heap-based buffer overflows, as demonstrated using MRBP16::bCheckRecord.

CVE-2005-2123 has been assigned by secure@microsoft.com 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
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-2348
US-CERT Technical Cyber Security Alert TA05-312A -- Microsoft Windows Image Processing Vulnerabilities	US Government Resource www.us-cert.gov text/html	CERT TA05-312A
Secunia - Advisories - Avaya Products Microsoft Windows WMF/EMF Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 17461
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1263
Network Security, Vulnerability Assessment,	Patch	MISC

Intrusion Prevention	Vendor Advisory www.eeye.com text/html	www.eeye.com/html/research/advisories/AD20051108b.html
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1175
US-CERT Vulnerability Note VU#300549	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#300549
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:701
	support.avaya.com application/pdf	CONFIRM support.avaya.com/elmodocs2/security/ASA-2005-228.pdf
Secunia - Advisories - Microsoft Windows WMF/EMF File Rendering Arbitrary Code Execution	web.archive.org text/html	SECUNIA 17498
Microsoft Security Bulletin MS05-053 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS05-053
Microsoft Windows Graphics Rendering Engine WMF/EMF Format Code Execution Vulnerability	cve.report (archive) text/html	BID 15352
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1546
Secunia - Advisories - Nortel Centrex IP Client Manager Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 17223
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1063
SecurityTracker.com Archives - Microsoft Windows Buffer Overflows in Graphics Rendering Engine Lets Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTRACK 1015168

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	fr
Operating System	Microsoft	Windows 2000	All	sp4	All	fr
Operating System	Microsoft	Windows 2003 Server	64-bit	All	All	All
Operating	Microsoft	Windows 2003 Server	itanium	All	All	All

System						
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	itanium	All
Operating System	Microsoft	Windows 2003 Server	64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	itanium	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	itanium	All
Operating System	Microsoft	Windows Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	sp1	tablet_pc	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	sp1	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All

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

cpe:2.3:o:microsoft:windows_2003_server:itanium:*:*:*:*:*:*:*:

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

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

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

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

cpe:2.3:o:microsoft:windows_2003_server:itanium:*:*:*:*:*:*:*:

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

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

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

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→