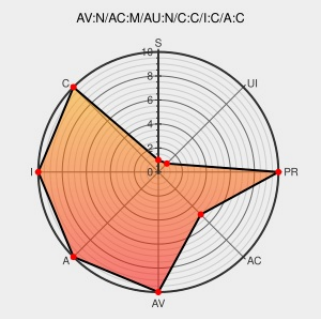
CVE-2008-2249

Published on: 12/10/2008 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:21 PM UTC

CVE-2008-2249

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



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

Integer overflow in GDI in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to execute arbitrary code via a malformed header in a crafted WMF file, which triggers a buffer overflow, aka "GDI Integer Overflow Vulnerability."

CVE-2008-2249 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:5984
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2008-3383
Microsoft Security Bulletin MS08-071 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS08-071
Microsoft GDI Buffer Overflows in Processing WMF Files Lets Remote Users Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1021365
Public Advisory: 12.09.08 // iDefense Labs	web.archive.org text/html Inactive Link Not Archived	IDEFENSE 20081209 Microsoft Windows Graphics Device Interface Integer Overflow Vulnerability

US-CERT Technical Cyber Security Alert TA08-344A -- Microsoft Updates for Multiple Vulnerabilities

US Government Resource
www.us-cert.gov
text/xml

CERT TA08-344A

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

System						
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	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	gold	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	gold	All	All	All
Operating System	Microsoft	Windows Xp	All	All	pro_x64	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp2	pro_x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	All	All	pro_x64	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp2	pro_x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All

cpe:2.3:o:microsoft:windows_2000:*:sp4:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp4:*:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_2003_server:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:*:sp2:x64:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_2003_server:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:*:sp2:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:*:sp1:itanium:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:*:x64:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:*:sp1:itanium:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:*:x64:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:*:*:itanium:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:*:*:x32:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:*:*:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:*:*:itanium:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:*:*:x32:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:*:*:x64:*:*:*:*:*:

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_vista:gold:*:*:*:*:*:*:*:

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_vista:gold:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:*:pro_x64:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_xp:*:sp2:pro_x64:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_xp:*:*:pro_x64:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_xp:*:sp2:pro_x64:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→