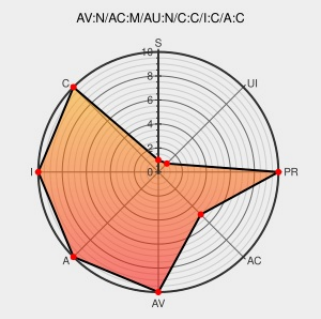
CVE-2011-0041

Published on: 04/13/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:19 PM UTC

CVE-2011-0041

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



Certain versions of Office from Microsoft contain the following vulnerability:

Integer overflow in gdiplus.dll in GDI+ in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold and SP2, and Office XP SP3 allows remote attackers to execute arbitrary code via a crafted EMF image, aka "GDI+ Integer Overflow Vulnerability."

CVE-2011-0041 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
Microsoft Security Bulletin MS11-029 - Critical | Microsoft Docs	docs.microsoft.com, text/html	MS MS11-029
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:11854
US-CERT Technical Cyber Security Alert TA11-102A -- Microsoft Updates for Multiple Vulnerabilities	US Government Resource, www.us-cert.gov, text/xml	CERT TA11-102A

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Office	xp	sp3	All	All
Application	Microsoft	Office	xp	sp3	All	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	All	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	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	sp2	x32	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	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	sp2	x32	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating	Microsoft	Windows Vista	All	sp2	All	All

System

Operating System	Microsoft	Windows Vista	All	sp2	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	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All

cpe:2.3:a:microsoft:office:xp:sp3:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:xp:sp3:*:*:*:*:*:*:

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

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

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

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

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:*:sp2:x32:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:*:sp2:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:itanium:*:*:*:*:*:

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:*:sp2:x32:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:*:sp2:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:itanium:*:*:*:*:*:

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

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

cpe:2.3:o:microsoft:windows_vista:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:sp2: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:*:sp2:*:*:*:*:*:*:

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

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→