



CVE-2013-3906

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2013-3906
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-11-06 15:55:00 UTC
Updated	2023-12-07 18:38:00 UTC
Description	GDI+ in Microsoft Windows Vista SP2 and Server 2008 SP2; Office 2003 SP3, 2007 SP3, and 2010 SP1 and SP2; Office C

Risk And Classification

EPSS: 0.926280000 probability, percentile 0.997430000 (date 2026-04-02)

CISA KEV: Listed on 2022-02-15; due 2022-08-15; ransomware use Unknown

Problem Types: CWE-94

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Graphics Component
Name	Microsoft Graphics Component Memory Corruption Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2013-3906

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Lync	2010	All	attendee	All
Application	Microsoft	Lync	2010	All	x64	All
Application	Microsoft	Lync	2010	All	x86	All
Application	Microsoft	Lync	2013	-	x64	All
Application	Microsoft	Lync	2013	-	x86	All
Application	Microsoft	Lync	2010	All	attendee	All
Application	Microsoft	Lync	2010	All	x64	All
Application	Microsoft	Lync	2010	All	x86	All

Application	Microsoft	Lync	2013	-	x64	All
Application	Microsoft	Lync	2013	-	x86	All
Application	Microsoft	Lync Basic	2013	-	x64	All
Application	Microsoft	Lync Basic	2013	-	x86	All
Application	Microsoft	Lync Basic	2013	-	x64	All
Application	Microsoft	Lync Basic	2013	-	x86	All
Application	Microsoft	Office	2003	sp3	All	All
Application	Microsoft	Office	2007	sp3	All	All
Application	Microsoft	Office	2010	sp1	x64	All
Application	Microsoft	Office	2010	sp1	x86	All
Application	Microsoft	Office	2010	sp2	x64	All
Application	Microsoft	Office	2010	sp2	x86	All
Application	Microsoft	Office	2003	sp3	All	All
Application	Microsoft	Office	2007	sp3	All	All
Application	Microsoft	Office	2010	sp1	x64	All
Application	Microsoft	Office	2010	sp1	x86	All
Application	Microsoft	Office	2010	sp2	x64	All
Application	Microsoft	Office	2010	sp2	x86	All
Operating System	Microsoft	Windows Server 2008	All	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x86	All
Operating System	Microsoft	Windows Server 2008	All	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x86	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All

References

Reference	S
McAfee Labs Detects Zero-Day Exploit Targeting Microsoft Office McAfee	M
Microsoft Tagged Image File Format (TIFF) Integer Overflow	E
Microsoft Security Advisory (2896666): Vulnerability in Microsoft Graphics Component Could Allow Remote Code Execution	C
CVE-2013-3906: a graphics vulnerability exploited through Word documents - Security Research & Defense - Site Home - TechNet Blogs	C

Microsoft Security Bulletin MS13-096 - Critical Microsoft Docs	N
CVE Program record	C
NVD vulnerability detail	N
CISA Known Exploited Vulnerabilities catalog	C

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)