



CVE-2009-1217

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2009-1217
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-04-01 18:00:00 UTC
Updated	2021-11-08 21:45:00 UTC
Description	Off-by-one error in the GpFont::SetData function in gdiplus.dll in Microsoft GDI+ on Windows XP allows remote attackers to

Risk And Classification

Problem Types: CWE-193

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Gdiplus	All	All	All	All
Operating System	Microsoft	Gdiplus	All	All	All	All
Application	Microsoft	Gdi	-	All	All	All
Operating System	Microsoft	Windows Xp	-	All	All	All
Operating System	Microsoft	Windows Xp	All	All	All	All
Operating System	Microsoft	Windows Xp	All	All	All	All

References

Reference	Source	Link
Microsoft GDI+ EMF 'GpFont.SetData()' Buffer Overflow Vulnerability	BID	www.securityfocus.com
[Black Security]: Microsoft GdiPlus EMF GpFont.SetData Integer Overflow	MISC	bl4cksecurity.blogspot.com
Security Research & Defense : New EMF gdiplus.dll crash not exploitable for code execution	CONFIRM	blogs.technet.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

Free CVE JSON API [cve.report/api](#)

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