



CVE-2005-0966

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

Summary

CVE	CVE-2005-0966
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-02 04:00:00 UTC
Updated	2018-10-19 15:31:00 UTC
Description	The IRC protocol plugin in Gaim 1.2.0, and possibly earlier versions, allows (1) remote attackers to inject arbitrary Gaim ma

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rob Flynn	Gaim	1.2.0	All	All	All
Application	Rob Flynn	Gaim	1.2.0	All	All	All

References

Reference	Source	Link	Tags
Secunia - Advisories - Gaim Multiple Denial of Service Weaknesses	SECUNIA	secunia.com	Patch, Vendor Adviso
Repository / Oval Repository	OVAL	oval.cisecurity.org	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Security Issues - Gaim	CONFIRM	gaim.sourceforge.net	Vendor Advisory
SourceForge.net: Pidgin: Files	CONFIRM	sourceforge.net	Patch
SecurityFocus	FEDORA	www.securityfocus.com	
Advisories - Mandriva	MANDRAKE	www.mandriva.com	
'multiple remote denial of service vulnerabilities in Gaim' - MARC	BUGTRAQ	marc.info	
Security Announcement	SUSE	www.novell.com	
Gaim IRC Protocol Plug-in Markup Language Injection Vulnerability	BID	www.securityfocus.com	
Support	REDHAT	www.redhat.com	

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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