



# CVE-2005-0472

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

## Summary

<b>CVE</b>	CVE-2005-0472
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-03-14 05:00:00 UTC
<b>Updated</b>	2018-10-19 15:31:00 UTC
<b>Description</b>	Gaim before 1.1.3 allows remote attackers to cause a denial of service (infinite loop) via malformed SNAC packets from (1)

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.0	All	amd64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.1	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.0	All	amd64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.1	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	3.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	3.0	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	3.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	3.0	All	x86_64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	enterprise_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	workstation	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	enterprise_server	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	workstation	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	4.0	All	All	All
Application	<a href="#">Rob Flynn</a>	<a href="#">Gaim</a>	1.0	All	All	All
Application	<a href="#">Rob Flynn</a>	<a href="#">Gaim</a>	1.0.1	All	All	All
Application	<a href="#">Rob Flynn</a>	<a href="#">Gaim</a>	1.1.1	All	All	All
Application	<a href="#">Rob Flynn</a>	<a href="#">Gaim</a>	1.1.2	All	All	All
Application	<a href="#">Rob Flynn</a>	<a href="#">Gaim</a>	1.0	All	All	All
Application	<a href="#">Rob Flynn</a>	<a href="#">Gaim</a>	1.0.1	All	All	All
Application	<a href="#">Rob Flynn</a>	<a href="#">Gaim</a>	1.1.1	All	All	All
Application	<a href="#">Rob Flynn</a>	<a href="#">Gaim</a>	1.1.2	All	All	All

## References

Reference	Source	Link	Tags
Security Issues - Gaim	CONFIRM	<a href="http://gaim.sourceforge.net">gaim.sourceforge.net</a>	Vendor Advisory
Debian -- Security Information -- DSA-716-1 gaim	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
'[USN-85-1] Gaim vulnerabilities' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>	
Gentoo Linux Documentation -- Gaim: Multiple Denial of Service issues	GENTOO	<a href="http://www.gentoo.org">www.gentoo.org</a>	
SecurityFocus	FEDORA	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
US-CERT Vulnerability Note VU#839280	CERT-VN	<a href="http://www.kb.cert.org">www.kb.cert.org</a>	Patch, Third Party
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	
rhn.redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>	
Security Announcement	SUSE	<a href="http://www.novell.com">www.novell.com</a>	
Secunia - Advisories - Gaim Two Denial of Service Weaknesses	SECUNIA	<a href="http://secunia.com">secunia.com</a>	
Advisories - Mandriva	MANDRAKE	<a href="http://www.mandriva.com">www.mandriva.com</a>	
Home - Conectiva	CONNECTIVA	<a href="http://distro.conectiva.com.br">distro.conectiva.com.br</a>	
Gaim Multiple Remote Denial of Service Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	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](#)**