



CVE-2004-0891

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

Summary

CVE	CVE-2004-0891
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-27 05:00:00 UTC
Updated	2017-10-11 01:29:00 UTC
Description	Buffer overflow in the MSN protocol handler for gaim 0.79 to 1.0.1 allows remote attackers to cause a denial of service (app

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Gentoo	Linux	All	All	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Operating System	Gentoo	Linux	All	All	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Application	Rob Flynn	Gaim	0.10	All	All	All
Application	Rob Flynn	Gaim	0.10.3	All	All	All
Application	Rob Flynn	Gaim	0.50	All	All	All
Application	Rob Flynn	Gaim	0.51	All	All	All
Application	Rob Flynn	Gaim	0.52	All	All	All
Application	Rob Flynn	Gaim	0.53	All	All	All
Application	Rob Flynn	Gaim	0.54	All	All	All
Application	Rob Flynn	Gaim	0.55	All	All	All
Application	Rob Flynn	Gaim	0.56	All	All	All
Application	Rob Flynn	Gaim	0.57	All	All	All
Application	Rob Flynn	Gaim	0.58	All	All	All
Application	Rob Flynn	Gaim	0.59	All	All	All
Application	Rob Flynn	Gaim	0.59.1	All	All	All

Application	Rob Flynn	Gaim	0.60	All	All	All
Application	Rob Flynn	Gaim	0.61	All	All	All
Application	Rob Flynn	Gaim	0.62	All	All	All
Application	Rob Flynn	Gaim	0.63	All	All	All
Application	Rob Flynn	Gaim	0.64	All	All	All
Application	Rob Flynn	Gaim	0.65	All	All	All
Application	Rob Flynn	Gaim	0.66	All	All	All
Application	Rob Flynn	Gaim	0.67	All	All	All
Application	Rob Flynn	Gaim	0.68	All	All	All
Application	Rob Flynn	Gaim	0.69	All	All	All
Application	Rob Flynn	Gaim	0.70	All	All	All
Application	Rob Flynn	Gaim	0.71	All	All	All
Application	Rob Flynn	Gaim	0.72	All	All	All
Application	Rob Flynn	Gaim	0.73	All	All	All
Application	Rob Flynn	Gaim	0.74	All	All	All
Application	Rob Flynn	Gaim	0.75	All	All	All
Application	Rob Flynn	Gaim	0.78	All	All	All
Application	Rob Flynn	Gaim	0.82	All	All	All
Application	Rob Flynn	Gaim	0.82.1	All	All	All
Application	Rob Flynn	Gaim	1.0	All	All	All
Application	Rob Flynn	Gaim	1.0.1	All	All	All
Application	Rob Flynn	Gaim	0.10	All	All	All
Application	Rob Flynn	Gaim	0.10.3	All	All	All
Application	Rob Flynn	Gaim	0.50	All	All	All
Application	Rob Flynn	Gaim	0.51	All	All	All
Application	Rob Flynn	Gaim	0.52	All	All	All
Application	Rob Flynn	Gaim	0.53	All	All	All
Application	Rob Flynn	Gaim	0.54	All	All	All
Application	Rob Flynn	Gaim	0.55	All	All	All
Application	Rob Flynn	Gaim	0.56	All	All	All
Application	Rob Flynn	Gaim	0.57	All	All	All
Application	Rob Flynn	Gaim	0.58	All	All	All
Application	Rob Flynn	Gaim	0.59	All	All	All
Application	Rob Flynn	Gaim	0.59.1	All	All	All
Application	Rob Flynn	Gaim	0.60	All	All	All

Application	Rob Flynn	Gaim	0.61	All	All	All
Application	Rob Flynn	Gaim	0.62	All	All	All
Application	Rob Flynn	Gaim	0.63	All	All	All
Application	Rob Flynn	Gaim	0.64	All	All	All
Application	Rob Flynn	Gaim	0.65	All	All	All
Application	Rob Flynn	Gaim	0.66	All	All	All
Application	Rob Flynn	Gaim	0.67	All	All	All
Application	Rob Flynn	Gaim	0.68	All	All	All
Application	Rob Flynn	Gaim	0.69	All	All	All
Application	Rob Flynn	Gaim	0.70	All	All	All
Application	Rob Flynn	Gaim	0.71	All	All	All
Application	Rob Flynn	Gaim	0.72	All	All	All
Application	Rob Flynn	Gaim	0.73	All	All	All
Application	Rob Flynn	Gaim	0.74	All	All	All
Application	Rob Flynn	Gaim	0.75	All	All	All
Application	Rob Flynn	Gaim	0.78	All	All	All
Application	Rob Flynn	Gaim	0.82	All	All	All
Application	Rob Flynn	Gaim	0.82.1	All	All	All
Application	Rob Flynn	Gaim	1.0	All	All	All
Application	Rob Flynn	Gaim	1.0.1	All	All	All
Operating System	Slackware	Slackware Linux	10.0	All	All	All
Operating System	Slackware	Slackware Linux	9.0	All	All	All
Operating System	Slackware	Slackware Linux	9.1	All	All	All
Operating System	Slackware	Slackware Linux	current	All	All	All
Operating System	Slackware	Slackware Linux	10.0	All	All	All
Operating System	Slackware	Slackware Linux	9.0	All	All	All
Operating System	Slackware	Slackware Linux	9.1	All	All	All
Operating System	Slackware	Slackware Linux	current	All	All	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ia64	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ppc	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ia64	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ppc	All

References

Reference	Source	Link	Tags
usn/usn-8-1 - Ubuntu Linux	UBUNTU	www.ubuntu.com	

rhn.redhat.com Red Hat Support	REDHAT	www.redhat.com	Vendor Advisory
Security Issues - gaim	CONFIRM	gaim.sourceforge.net	Vendor Advisory
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Repository / Oval Repository	OVAL	oval.cisecurity.org	
Gentoo Linux Documentation -- Gaim: Multiple vulnerabilities	GENTOO	www.gentoo.org	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
FLSA:2188	FEDORA	bugzilla.fedora.us	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

CVE.report and Source URL Uptime Status status.cve.report