



# CVE-2005-0208

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

## Summary

<b>CVE</b>	CVE-2005-0208
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-05-02 04:00:00 UTC
<b>Updated</b>	2018-10-19 15:31:00 UTC
<b>Description</b>	The HTML parsing functions in Gaim before 1.1.4 allow remote attackers to cause a denial of service (application crash) via

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Rob Flynn</a>	<a href="#">Gaim</a>	1.1.0	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>	1.1.3	All	All	All
Application	<a href="#">Rob Flynn</a>	<a href="#">Gaim</a>	1.1.0	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>	1.1.3	All	All	All

## References

Reference	Source	Link	Tags
US-CERT Vulnerability Note VU#795812	CERT-VN	<a href="http://www.kb.cert.org">www.kb.cert.org</a>	Patch, Third Party Ad
'[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>	Patch, Vendor Advise
Security Issues - Gaim	CONFIRM	<a href="http://gaim.sourceforge.net">gaim.sourceforge.net</a>	Vendor Advisory
SecurityFocus	FEDORA	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	Patch, Vendor Advise

Gaim Remote Denial of Service Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
Security Announcement	SUSE	<a href="http://www.novell.com">www.novell.com</a>	
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</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>	Patch
Secunia - Advisories - Gaim HTML Processing Denial of Service Weakness	SECUNIA	<a href="http://secunia.com">secunia.com</a>	Patch, Vendor Adviso
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](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)