



CVE-2013-6487

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

Summary

CVE	CVE-2013-6487
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-06 17:00:00 UTC
Updated	2016-12-22 02:59:00 UTC
Description	Integer overflow in libpurple/protocols/gg/lib/http.c in the Gadu-Gadu (gg) parser in Pidgin before 2.10.8 allows remote attac

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pidgin	Pidgin	2.0.0	All	All	All
Application	Pidgin	Pidgin	2.0.1	All	All	All
Application	Pidgin	Pidgin	2.0.2	All	All	All
Application	Pidgin	Pidgin	2.0.2	All	linux	All
Application	Pidgin	Pidgin	2.1.0	All	All	All
Application	Pidgin	Pidgin	2.1.1	All	All	All
Application	Pidgin	Pidgin	2.10.0	All	All	All
Application	Pidgin	Pidgin	2.10.1	All	All	All
Application	Pidgin	Pidgin	2.10.2	All	All	All
Application	Pidgin	Pidgin	2.10.3	All	All	All
Application	Pidgin	Pidgin	2.10.4	All	All	All
Application	Pidgin	Pidgin	2.10.5	All	All	All
Application	Pidgin	Pidgin	2.10.6	All	All	All
Application	Pidgin	Pidgin	2.0.0	All	All	All
Application	Pidgin	Pidgin	2.0.1	All	All	All
Application	Pidgin	Pidgin	2.0.2	All	All	All
Application	Pidgin	Pidgin	2.0.2	All	linux	All

Application	Pidgin	Pidgin	2.1.0	All	All	All
Application	Pidgin	Pidgin	2.1.1	All	All	All
Application	Pidgin	Pidgin	2.10.0	All	All	All
Application	Pidgin	Pidgin	2.10.1	All	All	All
Application	Pidgin	Pidgin	2.10.2	All	All	All
Application	Pidgin	Pidgin	2.10.3	All	All	All
Application	Pidgin	Pidgin	2.10.4	All	All	All
Application	Pidgin	Pidgin	2.10.5	All	All	All
Application	Pidgin	Pidgin	2.10.6	All	All	All
Application	Pidgin	Pidgin	All	All	All	All

References						
Reference		Source	Link	Tags		
Gentoo Security		GENTOO	security.gentoo.org			
pidgin/main: changeset ec15aa187aa0		CONFIRM	hg.pidgin.im	Vendor		
openSUSE-SU-2014:0326-1: moderate: update for pidgin		SUSE	lists.opensuse.org			
Mageia Advisory: MGASA-2014-0074 - Updated libgadu packages fix security vulnerability		CONFIRM	advisories.mageia.org			
libgadu 1.11.3		MISC	libgadu.net			
[SECURITY] Fedora 20 Update: libgadu-1.12.0-0.3.rc2.fc20		FEDORA	lists.fedoraproject.org			
VRT: VRT-2013-1001 (CVE-2013-6487): Buffer overflow in Gadu-Gadu HTTP parsing		MISC	vrt-blog.snort.org			
Debian -- Security Information -- DSA-2859-1 pidgin		DEBIAN	www.debian.org			
Pidgin Security Advisories		CONFIRM	www.pidgin.im	Vendor		
USN-2101-1: libgadu vulnerability Ubuntu		UBUNTU	www.ubuntu.com			
Support / Security / Advisories / / MDVSA-2014:039 Mandriva		MANDRIVA	www.mandriva.com			
Pidgin 'gg_http_watch_fd()' Function Buffer Overflow Vulnerability		BID	www.securityfocus.com			
Debian -- Security Information -- DSA-2852-1 libgadu		DEBIAN	www.debian.org			
openSUSE-SU-2014:0239-1: moderate: update for pidgin, pidgin-branding-op		SUSE	lists.opensuse.org			
USN-2100-1: Pidgin vulnerabilities Ubuntu		UBUNTU	www.ubuntu.com			
Red Hat Customer Portal		REDHAT	rhn.redhat.com			
CVE Program record		CVE.ORG	www.cve.org	canonic		
NVD vulnerability detail		NVD	nvd.nist.gov	canonic		

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](#)