



CVE-2013-6489

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

Summary

CVE	CVE-2013-6489
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-06 17:00:00 UTC
Updated	2014-03-08 05:11:00 UTC
Description	Integer signedness error in the MXit functionality in Pidgin before 2.10.8 allows remote attackers to cause a denial of service

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	2.1.0	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	2.2.0	All	All	All
Application	Pidgin	Pidgin	2.2.1	All	All	All
Application	Pidgin	Pidgin	2.2.2	All	All	All
Application	Pidgin	Pidgin	2.3.0	All	All	All
Application	Pidgin	Pidgin	2.3.1	All	All	All

Application	Pidgin	Pidgin	2.4.0	All	All	All
Application	Pidgin	Pidgin	2.4.1	All	All	All
Application	Pidgin	Pidgin	2.4.2	All	All	All
Application	Pidgin	Pidgin	2.4.3	All	All	All
Application	Pidgin	Pidgin	2.5.0	All	All	All
Application	Pidgin	Pidgin	2.5.1	All	All	All
Application	Pidgin	Pidgin	2.5.2	All	All	All
Application	Pidgin	Pidgin	2.5.3	All	All	All
Application	Pidgin	Pidgin	2.5.4	All	All	All
Application	Pidgin	Pidgin	2.5.5	All	All	All
Application	Pidgin	Pidgin	2.5.6	All	All	All
Application	Pidgin	Pidgin	2.5.7	All	All	All
Application	Pidgin	Pidgin	2.5.8	All	All	All
Application	Pidgin	Pidgin	2.5.9	All	All	All
Application	Pidgin	Pidgin	2.6.0	All	All	All
Application	Pidgin	Pidgin	2.6.1	All	All	All
Application	Pidgin	Pidgin	2.6.2	All	All	All
Application	Pidgin	Pidgin	2.6.3	All	All	All
Application	Pidgin	Pidgin	2.6.4	All	All	All
Application	Pidgin	Pidgin	2.6.5	All	All	All
Application	Pidgin	Pidgin	2.6.6	All	All	All
Application	Pidgin	Pidgin	2.7.0	All	All	All
Application	Pidgin	Pidgin	2.7.1	All	All	All
Application	Pidgin	Pidgin	2.7.10	All	All	All
Application	Pidgin	Pidgin	2.7.11	All	All	All
Application	Pidgin	Pidgin	2.7.2	All	All	All
Application	Pidgin	Pidgin	2.7.3	All	All	All
Application	Pidgin	Pidgin	2.7.4	All	All	All
Application	Pidgin	Pidgin	2.7.5	All	All	All
Application	Pidgin	Pidgin	2.7.6	All	All	All
Application	Pidgin	Pidgin	2.7.7	All	All	All
Application	Pidgin	Pidgin	2.7.8	All	All	All
Application	Pidgin	Pidgin	2.7.9	All	All	All
Application	Pidgin	Pidgin	2.8.0	All	All	All
Application	Pidgin	Pidgin	2.9.0	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	2.1.0	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	2.2.0	All	All	All
Application	Pidgin	Pidgin	2.2.1	All	All	All
Application	Pidgin	Pidgin	2.2.2	All	All	All
Application	Pidgin	Pidgin	2.3.0	All	All	All
Application	Pidgin	Pidgin	2.3.1	All	All	All
Application	Pidgin	Pidgin	2.4.0	All	All	All
Application	Pidgin	Pidgin	2.4.1	All	All	All
Application	Pidgin	Pidgin	2.4.2	All	All	All
Application	Pidgin	Pidgin	2.4.3	All	All	All
Application	Pidgin	Pidgin	2.5.0	All	All	All
Application	Pidgin	Pidgin	2.5.1	All	All	All
Application	Pidgin	Pidgin	2.5.2	All	All	All
Application	Pidgin	Pidgin	2.5.3	All	All	All
Application	Pidgin	Pidgin	2.5.4	All	All	All
Application	Pidgin	Pidgin	2.5.5	All	All	All
Application	Pidgin	Pidgin	2.5.6	All	All	All
Application	Pidgin	Pidgin	2.5.7	All	All	All
Application	Pidgin	Pidgin	2.5.8	All	All	All
Application	Pidgin	Pidgin	2.5.9	All	All	All
Application	Pidgin	Pidgin	2.6.0	All	All	All
Application	Pidgin	Pidgin	2.6.1	All	All	All
Application	Pidgin	Pidgin	2.6.2	All	All	All
Application	Pidgin	Pidgin	2.6.3	All	All	All
Application	Pidgin	Pidgin	2.6.4	All	All	All

Application	Pidgin	Pidgin	2.6.4	All	All	All
Application	Pidgin	Pidgin	2.6.5	All	All	All
Application	Pidgin	Pidgin	2.6.6	All	All	All
Application	Pidgin	Pidgin	2.7.0	All	All	All
Application	Pidgin	Pidgin	2.7.1	All	All	All
Application	Pidgin	Pidgin	2.7.10	All	All	All
Application	Pidgin	Pidgin	2.7.11	All	All	All
Application	Pidgin	Pidgin	2.7.2	All	All	All
Application	Pidgin	Pidgin	2.7.3	All	All	All
Application	Pidgin	Pidgin	2.7.4	All	All	All
Application	Pidgin	Pidgin	2.7.5	All	All	All
Application	Pidgin	Pidgin	2.7.6	All	All	All
Application	Pidgin	Pidgin	2.7.7	All	All	All
Application	Pidgin	Pidgin	2.7.8	All	All	All
Application	Pidgin	Pidgin	2.7.9	All	All	All
Application	Pidgin	Pidgin	2.8.0	All	All	All
Application	Pidgin	Pidgin	2.9.0	All	All	All
Application	Pidgin	Pidgin	All	All	All	All

References			
Reference	Source	Link	Tags
Pidgin Security Advisories	CONFIRM	www.pidgin.im	Vendor Advisory
Debian -- Security Information -- DSA-2859-1 pidgin	DEBIAN	www.debian.org	
Pidgin 'asn_getUtf8()' Function Buffer Overflow Vulnerability	BID	www.securityfocus.com	
pidgin/main: changeset 4c897372b5a4	MISC	hg.pidgin.im	
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	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.

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