



CVE-2013-6483

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

Summary

CVE	CVE-2013-6483
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-06 16:10:00 UTC
Updated	2014-03-16 04:42:00 UTC
Description	The XMPP protocol plugin in libpurple in Pidgin before 2.10.8 does not properly determine whether the from address in an i

Risk And Classification

Problem Types: CWE-20

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/main: changeset 93d4bff19574	CONFIRM	hg.pidgin.im	
Pidgin Security Advisories	CONFIRM	pidgin.im	Vendor Advisory
openSUSE-SU-2014:0326-1: moderate: update for pidgin	SUSE	lists.opensuse.org	
Debian -- Security Information -- DSA-2859-1 pidgin	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	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.

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](#)