



CVE-2009-2694

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

Summary

CVE	CVE-2009-2694
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-21 11:02:00 UTC
Updated	2017-09-19 01:29:00 UTC
Description	The msn_slplink_process_msg function in libpurple/protocols/msn/slplink.c in libpurple, as used in Pidgin (formerly Gaim) b

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adium	Adium	1.2.7	All	All	All
Application	Adium	Adium	1.3	All	All	All
Application	Adium	Adium	1.3.1	All	All	All
Application	Adium	Adium	1.3.2	All	All	All
Application	Adium	Adium	1.3.3	All	All	All
Application	Adium	Adium	1.3.4	All	All	All
Application	Adium	Adium	1.2.7	All	All	All
Application	Adium	Adium	1.3	All	All	All
Application	Adium	Adium	1.3.1	All	All	All
Application	Adium	Adium	1.3.2	All	All	All
Application	Adium	Adium	1.3.3	All	All	All
Application	Adium	Adium	1.3.4	All	All	All
Application	Adium	Adium	All	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	2.2.0	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	2.5.6	All	All	All
Application	Pidgin	Pidgin	2.5.7	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	2.2.0	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	2.5.6	All	All	All
Application	Pidgin	Pidgin	2.5.7	All	All	All
Application	Pidgin	Pidgin	All	All	All	All

References						
Reference						Source
Pidgin "msn_slplink_process_msg()" Memory Corruption Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com						SECUNIA
Gentoo update for pidgin - Secunia.com						SECUNIA
Pidgin Security Advisories						CONFIRMED
rhn.redhat.com Red Hat Support						REDHAT
Debian -- Security Information -- DSA-1870-1 pidgin						DEBIAN
Red Hat update for pidgin - Secunia Advisories - Vulnerability Information - Secunia.com						SECUNIA
Security Advisory SA36708 - Sun Solaris Pidgin Buffer Overflow Vulnerability - Secunia						SECUNIA
404 Not Found						CONFIRMED
ChangeLog – Pidgin – Trac						CONFIRMED
Adium "msn_slplink_process_msg()" Memory Corruption Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com						SECUNIA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUPEL
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUPEL
Core Security Technologies						MISC
Repository / Oval Repository						OVAL
266908						SUNALERT
Bug 514957 – CVE-2009-2694 pidgin: insufficient input validation in msn_slplink_process_msg()						CONFIRMED
Pidgin MSN <= 2.5.8 Remote Code Execution Exploit						EXPLOIT
Debian update for pidgin - Secunia.com						SECUNIA
Repository / Oval Repository						OVAL
CVE Program record						CVE.COM
NVD vulnerability detail						NVD

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