CVE-2011-1091

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2011-1091
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-03-14 19:55:00 UTC
Updated	2023-02-13 04:29:00 UTC
Description	libymsg.c in the Yahoo! protocol plugin in libpurple in Pidgin 2.6.0 through 2.7.10 allows (1) remote authenticated users to c

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	2.6.4	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	2.7.2	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	2.6.0	All	All	All
Application	Pidgin	Pidgin	2.6.1	All	All	All
Application	Pidgin	Pidgin	2.6.2	All	All	All
Application	Pidgin	Pidgin	2.6.4	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	2.7.2	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

References

Reference	Source	Lin
[SECURITY] Fedora 14 Update: pidgin-2.7.11-1.fc14	FEDORA	lists
IBM X-Force Exchange	XF	exc
Repository / Oval Repository	OVAL	ova
Hermes - openSUSE Notification Client	SUSE	her
683031 – (CVE-2011-1091) CVE-2011-1091 Pidgin: Multiple NULL pointer dereference flaws in Yahoo protocol plug-in	CONFIRM	bug
404 Not Found	CONFIRM	dev
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	ww
Red Hat update for pidgin - Secunia.com	SECUNIA	sec
404 Not Found	CONFIRM	dev
Pidgin YMSG Denial of Service Weakness - Advisories - Community	SECUNIA	sec
Support	REDHAT	ww
Pidgin Security Advisories	CONFIRM	ww
Support	REDHAT	ww
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	ww
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	ww

[SECURITY] Fedora 15 Update: pidgin-2.7.11-1.fc15	FEDORA	lists
access.redhat.com | CVE-2011-1091	MISC	acc
Libpurple Yahoo Protocol 'YMSG' NULL Pointer Dereference Denial of Service Vulnerability	BID	ww
Fedora update for pidgin - Secunia.com	SECUNIA	sec
Red Hat Customer Portal	MISC	acc
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	ww
Red Hat Customer Portal	MISC	acc
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	sla
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

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 registred 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**