



CVE-2011-1178

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

Summary

CVE	CVE-2011-1178
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-06-06 19:55:00 UTC
Updated	2023-02-13 04:29:00 UTC
Description	Multiple integer overflows in the load_image function in file-pcx.c in the Personal Computer Exchange (PCX) plugin in GIMP

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gimp	Gimp	2.6.8	All	All	All
Application	Gimp	Gimp	2.6.8	All	All	All
Application	Gimp	Gimp	All	All	All	All
Application	Gimp	Gimp	All	All	All	All
Application	Gnu	Gimp	1.0.4	All	All	All
Application	Gnu	Gimp	1.2.5	All	All	All
Application	Gnu	Gimp	2.0.0	All	All	All
Application	Gnu	Gimp	2.0.1	All	All	All
Application	Gnu	Gimp	2.0.2	All	All	All
Application	Gnu	Gimp	2.0.3	All	All	All
Application	Gnu	Gimp	2.0.4	All	All	All
Application	Gnu	Gimp	2.0.5	All	All	All
Application	Gnu	Gimp	2.0.6	All	All	All
Application	Gnu	Gimp	2.2.0	All	All	All
Application	Gnu	Gimp	2.2.1	All	All	All
Application	Gnu	Gimp	2.2.10	All	All	All
Application	Gnu	Gimp	2.2.11	All	All	All

Application	Gnu	Gimp	2.2.12	All	All	All
Application	Gnu	Gimp	2.2.13	All	All	All
Application	Gnu	Gimp	2.2.14	All	All	All
Application	Gnu	Gimp	2.2.15	All	All	All
Application	Gnu	Gimp	2.2.16	All	All	All
Application	Gnu	Gimp	2.2.17	All	All	All
Application	Gnu	Gimp	2.2.2	All	All	All
Application	Gnu	Gimp	2.2.3	All	All	All
Application	Gnu	Gimp	2.2.4	All	All	All
Application	Gnu	Gimp	2.2.5	All	All	All
Application	Gnu	Gimp	2.2.6	All	All	All
Application	Gnu	Gimp	2.2.7	All	All	All
Application	Gnu	Gimp	2.2.8	All	All	All
Application	Gnu	Gimp	2.2.9	All	All	All
Application	Gnu	Gimp	2.4.0	All	All	All
Application	Gnu	Gimp	2.4.1	All	All	All
Application	Gnu	Gimp	2.4.2	All	All	All
Application	Gnu	Gimp	2.4.3	All	All	All
Application	Gnu	Gimp	2.4.4	All	All	All
Application	Gnu	Gimp	2.4.5	All	All	All
Application	Gnu	Gimp	2.4.6	All	All	All
Application	Gnu	Gimp	2.4.7	All	All	All
Application	Gnu	Gimp	2.6.0	All	All	All
Application	Gnu	Gimp	2.6.1	All	All	All
Application	Gnu	Gimp	2.6.10	All	All	All
Application	Gnu	Gimp	2.6.2	All	All	All
Application	Gnu	Gimp	2.6.3	All	All	All
Application	Gnu	Gimp	2.6.4	All	All	All
Application	Gnu	Gimp	2.6.5	All	All	All
Application	Gnu	Gimp	2.6.6	All	All	All
Application	Gnu	Gimp	2.6.7	All	All	All
Application	Gnu	Gimp	2.6.9	All	All	All
Application	Gnu	Gimp	1.0.4	All	All	All
Application	Gnu	Gimp	1.2.5	All	All	All
Application	Gnu	Gimp	2.0.0	All	All	All

Application	Gnu	Gimp	2.0.1	All	All	All
Application	Gnu	Gimp	2.0.2	All	All	All
Application	Gnu	Gimp	2.0.3	All	All	All
Application	Gnu	Gimp	2.0.4	All	All	All
Application	Gnu	Gimp	2.0.5	All	All	All
Application	Gnu	Gimp	2.0.6	All	All	All
Application	Gnu	Gimp	2.2.0	All	All	All
Application	Gnu	Gimp	2.2.1	All	All	All
Application	Gnu	Gimp	2.2.10	All	All	All
Application	Gnu	Gimp	2.2.11	All	All	All
Application	Gnu	Gimp	2.2.12	All	All	All
Application	Gnu	Gimp	2.2.13	All	All	All
Application	Gnu	Gimp	2.2.14	All	All	All
Application	Gnu	Gimp	2.2.15	All	All	All
Application	Gnu	Gimp	2.2.16	All	All	All
Application	Gnu	Gimp	2.2.17	All	All	All
Application	Gnu	Gimp	2.2.2	All	All	All
Application	Gnu	Gimp	2.2.3	All	All	All
Application	Gnu	Gimp	2.2.4	All	All	All
Application	Gnu	Gimp	2.2.5	All	All	All
Application	Gnu	Gimp	2.2.6	All	All	All
Application	Gnu	Gimp	2.2.7	All	All	All
Application	Gnu	Gimp	2.2.8	All	All	All
Application	Gnu	Gimp	2.2.9	All	All	All
Application	Gnu	Gimp	2.4.0	All	All	All
Application	Gnu	Gimp	2.4.1	All	All	All
Application	Gnu	Gimp	2.4.2	All	All	All
Application	Gnu	Gimp	2.4.3	All	All	All
Application	Gnu	Gimp	2.4.4	All	All	All
Application	Gnu	Gimp	2.4.5	All	All	All
Application	Gnu	Gimp	2.4.6	All	All	All
Application	Gnu	Gimp	2.4.7	All	All	All
Application	Gnu	Gimp	2.6.0	All	All	All
Application	Gnu	Gimp	2.6.1	All	All	All
Application	Gnu	Gimp	2.6.10	All	All	All

Application	Gnu	Gimp	2.6.2	All	All	All
Application	Gnu	Gimp	2.6.3	All	All	All
Application	Gnu	Gimp	2.6.4	All	All	All
Application	Gnu	Gimp	2.6.5	All	All	All
Application	Gnu	Gimp	2.6.6	All	All	All
Application	Gnu	Gimp	2.6.7	All	All	All
Application	Gnu	Gimp	2.6.9	All	All	All

References

Reference	Source	Link
access.redhat.com CVE-2011-1178	MISC	access.r
GIMP Buffer Overflow in Processing PCX Image Files Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	securityt
689831 – (CVE-2011-1178) CVE-2011-1178 Gimp: Integer overflow in the PCX image file plug-in	CONFIRM	bugzilla.
Gentoo Linux Documentation -- GIMP: Multiple vulnerabilities	GENTOO	security.
IBM X-Force Exchange	XF	exchang
Red Hat Customer Portal	MISC	access.r
Support	REDHAT	www.rec
Security Alerts - Secunia	SECUNIA	secunia.
Support / Security / Advisories // MDVSA-2011:110 Mandriva	MANDRIVA	www.ma
Red Hat Customer Portal	MISC	access.r
Support	REDHAT	www.rec
PCX: Avoid allocation overflows. (a9671395) · Commits · GNOME / GIMP · GitLab	CONFIRM	git.gnom
GIMP PCX Image Parsing Heap Buffer Overflow Vulnerability	BID	www.se
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)

