



CVE-2006-3404

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

Summary

CVE	CVE-2006-3404
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-07-06 20:05:00 UTC
Updated	2022-02-07 17:27:00 UTC
Description	Buffer overflow in the xcf_load_vector function in app/xcf/xcf-load.c for gimp before 2.2.12 allows user-assisted attackers to

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gimp	Gimp	All	All	All	All
Application	The Gimp Team	Gimp	2.2.11	All	All	All
Application	The Gimp Team	Gimp	2.2.8	All	All	All
Application	The Gimp Team	Gimp	2.2.9	All	All	All
Application	The Gimp Team	Gimp	2.3.9	All	All	All
Application	The Gimp Team	Gimp	2.2.11	All	All	All
Application	The Gimp Team	Gimp	2.2.8	All	All	All
Application	The Gimp Team	Gimp	2.2.9	All	All	All
Application	The Gimp Team	Gimp	2.3.9	All	All	All
Application	The Gimp Team	Gimp	All	All	All	All

References

Reference	Source	Link
Bug 346742 – Buffer overrun in XCF parsing code	CONFIRM	bugzi
Mandriva update for gimp - Advisories - Secunia	SECUNIA	secur
Gimp XCF Parsing Buffer Overflow Vulnerability - Advisories - Secunia	SECUNIA	secur
Gentoo update for gimp - Advisories - Secunia	SECUNIA	secur

SecurityFocus	BUGTRAQ	www.
Ubuntu update for gimp - Advisories - Secunia	SECUNIA	secur
200070	SUNALERT	sunsc
102720	SUNALERT	sunsc
27037	OSVDB	www.
SecurityTracker.com Archives - GIMP Buffer Overflow in xcf_load_vector() Lets Remote Users Execute Arbitrary Code	SECTRACK	secur
IBM X-Force Exchange	XF	excha
rPath update for gimp - Advisories - Secunia	SECUNIA	secur
SecurityFocus	BUGTRAQ	www.
Sun Solaris Gimp XCF Parsing Buffer Overflow Vulnerability - Advisories - Secunia	SECUNIA	secur
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.
rh.n.redhat.com Red Hat Support	REDHAT	www.
[#RPL-522] gimp in rpl:1 potentially vulnerable to buffer overflow - rPath JIRA	CONFIRM	issue:
Repository / Oval Repository	OVAL	oval.c
Debian -- Security Information -- DSA-1116-1 gimp	DEBIAN	www.
Red Hat update for gimp - Advisories - Secunia	SECUNIA	secur
SUSE Updates for Multiple Packages - Advisories - Secunia	SECUNIA	secur
#377049 - gimp: Buffer overrun in XCF reading code - Debian Bug report logs	MISC	bugs.
Repository / Oval Repository	OVAL	oval.c
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.
Advisories - Mandriva Linux	MANDRIVA	www.
Gentoo Linux Documentation -- GIMP: Buffer overflow	GENTOO	secur
SecurityFocus	BUGTRAQ	www.
Security Announcement	SUSE	www.
Gimp XCF_load_vector Function Buffer Overflow Vulnerability	BID	www.
usn/usn-312-1 - Ubuntu: Linux for human beings	UBUNTU	www.
Debian update for gimp - Advisories - Secunia	SECUNIA	secur
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

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](#)