



CVE-2009-5018

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

Summary

CVE	CVE-2009-5018
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-14 17:00:00 UTC
Updated	2017-08-17 01:31:00 UTC
Description	Stack-based buffer overflow in gif2png.c in gif2png 2.5.3 and earlier might allow context-dependent attackers to execute ar

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Catb	Gif2png	0.99	All	All	All
Application	Catb	Gif2png	1.0.0	All	All	All
Application	Catb	Gif2png	1.1.0	All	All	All
Application	Catb	Gif2png	1.1.1	All	All	All
Application	Catb	Gif2png	1.2.0	All	All	All
Application	Catb	Gif2png	1.2.1	All	All	All
Application	Catb	Gif2png	1.2.2	All	All	All
Application	Catb	Gif2png	2.0.0	All	All	All
Application	Catb	Gif2png	2.0.1	All	All	All
Application	Catb	Gif2png	2.0.2	All	All	All
Application	Catb	Gif2png	2.0.3	All	All	All
Application	Catb	Gif2png	2.1.1	All	All	All
Application	Catb	Gif2png	2.1.2	All	All	All
Application	Catb	Gif2png	2.1.3	All	All	All
Application	Catb	Gif2png	2.2.0	All	All	All
Application	Catb	Gif2png	2.2.1	All	All	All
Application	Catb	Gif2png	2.2.2	All	All	All

Application	Catb	Gif2png	2.2.3	All	All	All
Application	Catb	Gif2png	2.2.4	All	All	All
Application	Catb	Gif2png	2.2.5	All	All	All
Application	Catb	Gif2png	2.3.0	All	All	All
Application	Catb	Gif2png	2.3.1	All	All	All
Application	Catb	Gif2png	2.3.2	All	All	All
Application	Catb	Gif2png	2.3.3	All	All	All
Application	Catb	Gif2png	2.4.0	All	All	All
Application	Catb	Gif2png	2.4.1	All	All	All
Application	Catb	Gif2png	2.4.2	All	All	All
Application	Catb	Gif2png	2.4.3	All	All	All
Application	Catb	Gif2png	2.4.4	All	All	All
Application	Catb	Gif2png	2.4.5	All	All	All
Application	Catb	Gif2png	2.4.6	All	All	All
Application	Catb	Gif2png	2.4.7	All	All	All
Application	Catb	Gif2png	2.5.0	All	All	All
Application	Catb	Gif2png	2.5.1	All	All	All
Application	Catb	Gif2png	2.5.2	All	All	All
Application	Catb	Gif2png	0.99	All	All	All
Application	Catb	Gif2png	1.0.0	All	All	All
Application	Catb	Gif2png	1.1.0	All	All	All
Application	Catb	Gif2png	1.1.1	All	All	All
Application	Catb	Gif2png	1.2.0	All	All	All
Application	Catb	Gif2png	1.2.1	All	All	All
Application	Catb	Gif2png	1.2.2	All	All	All
Application	Catb	Gif2png	2.0.0	All	All	All
Application	Catb	Gif2png	2.0.1	All	All	All
Application	Catb	Gif2png	2.0.2	All	All	All
Application	Catb	Gif2png	2.0.3	All	All	All
Application	Catb	Gif2png	2.1.1	All	All	All
Application	Catb	Gif2png	2.1.2	All	All	All
Application	Catb	Gif2png	2.1.3	All	All	All
Application	Catb	Gif2png	2.2.0	All	All	All
Application	Catb	Gif2png	2.2.1	All	All	All
Application	Catb	Gif2png	2.2.2	All	All	All

Application	Catb	Gif2png	2.2.3	All	All	All
Application	Catb	Gif2png	2.2.4	All	All	All
Application	Catb	Gif2png	2.2.5	All	All	All
Application	Catb	Gif2png	2.3.0	All	All	All
Application	Catb	Gif2png	2.3.1	All	All	All
Application	Catb	Gif2png	2.3.2	All	All	All
Application	Catb	Gif2png	2.3.3	All	All	All
Application	Catb	Gif2png	2.4.0	All	All	All
Application	Catb	Gif2png	2.4.1	All	All	All
Application	Catb	Gif2png	2.4.2	All	All	All
Application	Catb	Gif2png	2.4.3	All	All	All
Application	Catb	Gif2png	2.4.4	All	All	All
Application	Catb	Gif2png	2.4.5	All	All	All
Application	Catb	Gif2png	2.4.6	All	All	All
Application	Catb	Gif2png	2.4.7	All	All	All
Application	Catb	Gif2png	2.5.0	All	All	All
Application	Catb	Gif2png	2.5.1	All	All	All
Application	Catb	Gif2png	2.5.2	All	All	All
Application	Catb	Gif2png	All	All	All	All

References

Reference

oss-security - Re: CVE Request: gif2png: command-line buffer overflow problem

[Full-Disclosure] Mailing List Charter

Gentoo Linux Documentation -- gif2png: User-assisted execution of arbitrary code

oss-security - CVE Request: gif2png: command-line buffer overflow problem

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Support / Security / Advisories // MDVSA-2011:009 | Mandriva

Gentoo update for gif2png - Secunia.com

oss-security - Re: CVE Request: gif2png: command-line buffer overflow problem

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

IBM X-Force Exchange

547515 – (CVE-2009-5018, CVE-2010-4694, CVE-2010-4695) CVE-2009-5018 CVE-2010-4694, CVE-2010-4695 gif2png: command-line buff

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

gif2png Remote Buffer Overflow Vulnerability

#550978 - gif2png: Command line buffer overflow - Debian Bug report logs

[SECURITY] Fedora 12 Update: gif2png-2.5.1-1202.fc12

Bug 346501 – <media-gfx/gif2png-2.5.1-r1: Command Line Stack Overflow (CVE-2009-5018)

cvs.fedoraproject.org/viewvc/rpms/gif2png/devel/gif2png-overflow.patch

oss-security - Re: CVE Request: gif2png: command-line buffer overflow problem

CVE Program record

NVD vulnerability detail

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](#)