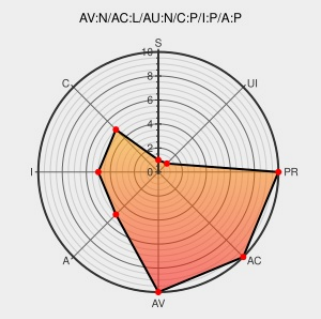
CVE-2010-4543

Published on: 01/07/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 03:20:00 AM UTC

CVE-2010-4543

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Gimp from Gimp contain the following vulnerability:

Heap-based buffer overflow in the read_channel_data function in file-psp.c in the Paint Shop Pro (PSP) plugin in GIMP 2.6.11 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a PSP_COMP_RLE (aka RLE compression) image file that begins a long run count at the end of the image. NOTE: some of these details are obtained from third party information.

CVE-2010-4543 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 70284
703407 – (CVE-2010-4543) CVE-2010-4543 Gimp: Heap-based buffer overflow in Paint Shop Pro (PSP) plug-in	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=703407
Red Hat update for gimp - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 44750
Gimp Multiple Vulnerabilities - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 42771

Debian -- Security Information -- DSA-2426-1 gimp	www.debian.org Depreciated Link text/html	DEBIAN DSA-2426
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2011:0839
Gentoo Linux Documentation -- GIMP: Multiple vulnerabilities	security.gentoo.org text/html	GENTOO GLSA-201209-23
CVE-2010-4543 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2010-4543
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2011:0838
Support	Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2011:0838
Security Alerts - Secunia	web.archive.org text/html	SECUNIA 50737
oss-security - Re: CVE request for buffer overflows in gimp	Exploit openwall.com text/html	MLIST [oss-security] 20110104 Re: CVE request for buffer overflows in gimp
Support	Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2011:0839
Security Advisory SA48236 - Debian update for gimp - Secunia	web.archive.org text/html	SECUNIA 48236
#608497 - gimp: four buffer overflows - Debian Bug report logs	Exploit bugs.debian.org text/html	MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=608497
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2011:0837
Support	www.redhat.com text/html	REDHAT RHSA-2011:0837
Support / Security / Advisories / / MDVSA-2011:103 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2011:103
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2011-0016
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:005	lists.opensuse.org text/html	SUSE SUSE-SR:2011:005
666793 – (CVE-2010-4540) CVE-2010-4540 Gimp: Stack-based buffer overflow in Lighting plug-in	Exploit bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=666793
oss-security - CVE request for buffer overflows in gimp	Exploit openwall.com text/html	MLIST [oss-security] 20110103 CVE request for buffer overflows in gimp

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gimp	Gimp	2.6.11	All	All	All
Application	Gimp	Gimp	2.6.11	All	All	All

cpe:2.3:a:gimp:gimp:2.6.11:*:*:*:*:*:*:*:

cpe:2.3:a:gimp:gimp:2.6.11:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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.

CVE.report and Source URL Uptime Status status.cve.report