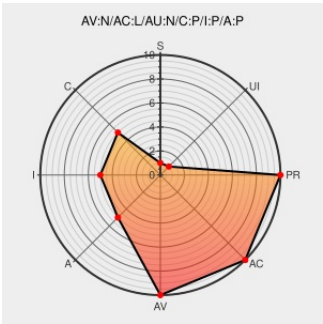
CVE-2011-1782

Published on: 07/26/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:19:00 AM UTC

CVE-2011-1782

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. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-4543.

CVE-2011-1782 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
Debian -- Security Information -- DSA-2426-1 gimp	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-2426
Bug 704512 – CVE-2011-1782 Gimp: Incomplete fix for CVE-2010-4543 PSP plug-in heap overflow issue	Patch, bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=704512
Security Advisory SA48236 - Debian update for gimp - Secunia	web.archive.org, text/html	SECUNIA 48236
Support / Security / Advisories / / MDVSA-2011:103 | Mandriva	www.mandriva.com, text/html	MANDRIVA MDVSA-2011:103

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→