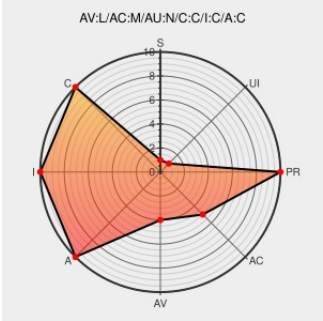
CVE-2008-4946

Published on: 11/05/2008 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:09 PM UTC

CVE-2008-4946

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



Certain versions of Convirt from Convirture contain the following vulnerability:

convirt 0.8.2 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/set_output temporary file, related to the (1) _template_/provision.sh, (2) Linux_CD_Install/provision.sh, (3) Fedora_PV_Install/provision.sh, (4) CentOS_PV_Install/provision.sh, (5) common/provision.sh, (6) example/provision.sh, and (7) Windows_CD_Install/provision.sh scripts in image_store/.

CVE-2008-4946 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
404 Not Found	Exploit, dev.gentoo.org, text/plain, Inactive Link, Not Archived	CONFIRM dev.gentoo.org/~rbu/security/debiantemp/convirt
235770 – (debian-tempfile) [Tracker] Tempfile issues found in Debian	bugs.gentoo.org, text/html	CONFIRM bugs.gentoo.org/show_bug.cgi?id=235770
oss-security - CVE requests: tempfile issues for aview, mgetty, openoffice, crossfire	www.openwall.com, text/html	MLIST [oss-security] 20081030 CVE requests: tempfile issues for aview, mgetty, openoffice, crossfire
#496419 - The possibility of attack with the help of symlinks in some Debian packages - Debian Bug report logs	bugs.debian.org, text/html	CONFIRM bugs.debian.org/496419

In some Debian packages - Debian Bug report logs

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	Convirture	Convirt	0.8.2	All	All	All
Application	Convirture	Convirt	0.8.2	All	All	All

cpe:2.3:a:convirture:convirt:0.8.2:*:*:*:*:*:*:*:

cpe:2.3:a:convirture:convirt:0.8.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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