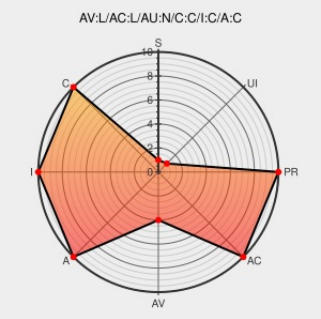
CVE-2004-2768

Published on: 06/08/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2768

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



Certain versions of Dpkg from Debian contain the following vulnerability:

dpkg 1.9.21 does not properly reset the metadata of a file during replacement of the file in a package upgrade, which might allow local users to gain privileges by creating a hard link to a vulnerable (1) setuid file, (2) setgid file, or (3) device, a related issue to CVE-2010-2059.

CVE-2004-2768 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF dpkg-setgid-privilege-escalation(59428)
#225692 - dpkg: Allows users to stash away vulnerable versions of setuid binaries - Debian Bug report logs	bugs.debian.org text/html	CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=225692
ISN 2003/12: [ISN] The mysteriously persistently exploitable pr	Exploit lists.jammed.com text/html	MLIST [isn] 20031215 The mysteriously persistently exploitable program explained.
Bug 598775 – CVE-2010-2059 rpm: fails to drop SUID/SGID bits on package upgrade	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=598775
Hacking Linux Exposed	Exploit www.hackinglinuxexposed.com text/html	MISC www.hackinglinuxexposed.com/articles/20031214.html

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	Debian	Dpkg	1.9.21	All	All	All
Application	Debian	Dpkg	1.9.21	All	All	All

cpe:2.3:a:debian:dpkg:1.9.21:*:*:*:*:*:*:*:

cpe:2.3:a:debian:dpkg:1.9.21:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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