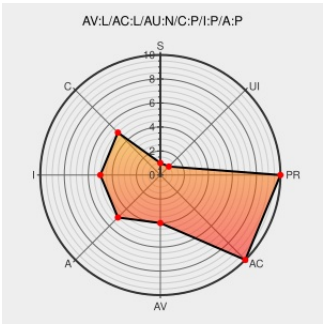
CVE-2010-4001

Published on: 11/05/2010 12:00:00 AM UTC

Last Modified on: 03/25/2021 11:02:28 PM UTC

CVE-2010-4001

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

** DISPUTED ** GMXRC.bash in Gromacs 4.5.1 and earlier places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse shared library in the current working directory. NOTE: CVE disputes this issue because the GMXLDLIB value is always added to the beginning of LD_LIBRARY_PATH at a later point in the script.

CVE-2010-4001 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
Bug 644596 – CVE-2010-4001 gromacs: insecure library loading vulnerability	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=644596
[SECURITY] Fedora 13 Update: gromacs-4.5.2-2.fc13	lists.fedoraproject.org text/html	FEDORA FEDORA-2010-17256
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	VUPEN ADV-2010-2971
[SECURITY] Fedora 14 Update: gromacs-4.5.2-2.fc14	lists.fedoraproject.org text/html	FEDORA FEDORA-2010-17248

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
Operating System	Fedoraproject	Fedora	All	All	All	All
Operating System	Fedoraproject	Fedora	All	All	All	All
Application	Gromacs	Gromacs	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:*:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:*:*:*:*:*:*:*:*:

cpe:2.3:a:gromacs:gromacs:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→