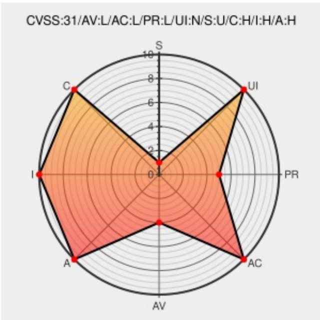
CVE-2008-3278

Published on: 11/07/2019 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:37 AM UTC

CVE-2008-3278

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



Certain versions of Enterprise Linux from Redhat contain the following vulnerability:

frysk packages through 2008-08-05 as shipped in Red Hat Enterprise Linux 5 are built with an insecure RPATH set in the ELF header of multiple binaries in /usr/bin/f* (e.g. fcore, fcatch, fstack, fstep, ...) shipped in the package. A local attacker can exploit this vulnerability by running arbitrary code as another user.

CVE-2008-3278 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **frysk** - **frysk** version **= through 2008-08-05**

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

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
457939 – (CVE-2008-3278) CVE-2008-3278 frysk: insecure	Issue Tracking	MISC bugzilla.redhat.com/show_bug.cgi?

relative RPATH	Vendor Advisory bugzilla.redhat.com text/html	id=CVE-2008-3278
CVE-2008-3278	Third Party Advisory security-tracker.debian.org text/html	MISC security-tracker.debian.org/tracker/CVE-2008-3278
CVE-2008-3278 - Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	MISC access.redhat.com/security/cve/cve-2008-3278

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
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Application	Redhat	Frysk	All	All	All	All

cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:frysk:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→