



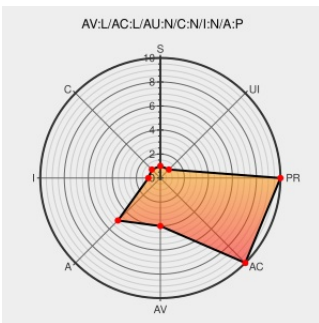
Last Modified on: 03/23/2021 11:27:32 PM UTC

CVE-1999-1331

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Linux](#) from [Redhat](#) contain the following vulnerability:

netcfg 2.16-1 in Red Hat Linux 4.2 allows the Ethernet interface to be controlled by users on reboot when an option is set, which allows local users to cause a denial of service by shutting down the interface.

CVE-1999-1331 has been assigned by  cve@mitre.org to track the vulnerability

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
ISS X-Force Database: netcfg-ethernet-dos (7245): netcfg in Linux allows other user to control ethernet device	web.archive.org text/html Inactive Link Not Archived	 XF netcfg-ethernet-dos(7245)
redhat.com Red Hat Support	www.redhat.com application/octet-stream	 CONFIRM www.redhat.com/support/errata/rh42-errata-general.html#netcfg

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	Linux	4.2	All	All	All
Operating System	Redhat	Linux	4.2	All	All	All
cpe:2.3:o:redhat:linux:4.2:*:*:*:*:*:						
cpe:2.3:o:redhat:linux:4.2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE