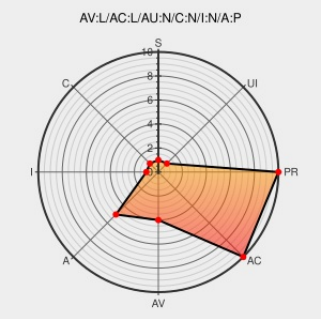
CVE-1999-1331

Published on: 12/31/1999 05:00:00 AM UTC

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

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

← Previous ID

Next ID→