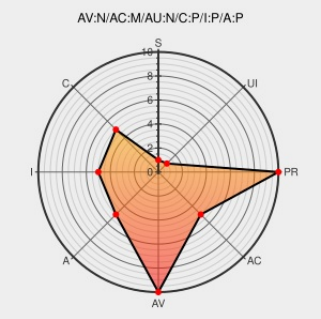
CVE-1999-0181

Published on: 01/01/1994 05:00:00 AM UTC

Last Modified on: 08/17/2022 07:15:00 AM UTC

CVE-1999-0181

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



Certain versions of Rpc.walld from Rpc.walld contain the following vulnerability:

The wall daemon can be used for denial of service, social engineering attacks, or to execute remote commands.

CVE-1999-0181 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	MISC exchange.xforce.ibmcloud.com/vulnerabilities/CVE-1999-0181

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	Rpc.walld	Rpc.walld	All	All	All	All
Application	Rpc.walld	Rpc.walld	All	All	All	All

cpe:2.3:a:rpc.walld:rpc.walld:*:*:*:*:*:*:*:*:

cpe:2.3:a:rpc.walld:rpc.walld:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→