

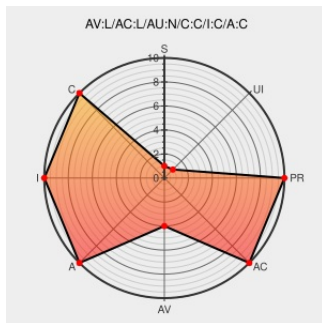


CVE-2004-1374

Published on: 12/18/2004 05:00:00 AM UTC

Last Modified on: 06/15/2021 12:00:00 AM UTC

CVE-2004-1374

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Multiple buffer overflows in NetBSD kernel may allow local users to execute arbitrary code and gain privileges.

CVE-2004-1374 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

GLEG: Advisories. NetBSD kernel local vulnerabilities

[Vendor Advisory](#)

[web.archive.org](#)

[text/html](#)

[Inactive Link](#)

[Not Archived](#)

[MISC gleg.net/advisory_netbsd2.shtml](https://gleg.net/advisory_netbsd2.shtml)

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)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Netbsd	Netbsd	2.0.4	All	All	All
Operating System	Netbsd	Netbsd	2.0.4	All	All	All
cpe:2.3:o:netbsd:netbsd:2.0.4:*****:.*						
cpe:2.3:o:netbsd:netbsd:2.0.4:*****:.*						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→