



CVE-2005-4741

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:21 PM UTC

CVE-2005-4741

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

NetBSD 1.6, NetBSD 2.0 through 2.1, and NetBSD-current before 20051031 allows local users to gain privileges by attaching a debugger to a setuid/setgid (P_SUGID) process that performs an exec without a reset of real credentials.

CVE-2005-4741 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

[ftp.netbsd.org](#)
[text/plain](#)

[NETBSD NetBSD-SA2005-013](#)

No Description Provided

[archives.neohapsis.com](#)
Inactive Link **Not Archived**

[FULLDISC 20051106](#)
[prdelka.blackart.org.uk/exploit/prdelka-vs-BSD-pttrace.tar.gz](#)

No Description Provided

[prdelka.blackart.org.uk](#)
Inactive Link **Not Archived**

[MISC prdelka.blackart.org.uk/exploit/prdelka-vs-BSD-pttrace.tar.gz](#)

source-changes: CVS commit: src/sys/kern

Patch
[mail-index.netbsd.org](#)
[text/html](#)

[CONFIRM mail-index.netbsd.org/source-changes/2005/10/31/0001.html](#)

No Description Provided

Vendor Advisory
[www.osvdb.org](#)

[OSVDB 20759](#)

Inactive Link Not Archived

NetBSD Local PTrace Privilege Escalation
Vulnerability

[cve.report \(archive\)](#)
[text/html](#)

 [BID 15290](#)

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	Netbsd	Netbsd	1.6	All	All	All
Operating System	Netbsd	Netbsd	1.6.1	All	All	All
Operating System	Netbsd	Netbsd	1.6.2	All	All	All
Operating System	Netbsd	Netbsd	2.0	All	All	All
Operating System	Netbsd	Netbsd	2.0.1	All	All	All
Operating System	Netbsd	Netbsd	2.0.2	All	All	All
Operating System	Netbsd	Netbsd	2.0.3	All	All	All
Operating System	Netbsd	Netbsd	2.1	All	All	All
Operating System	Netbsd	Netbsd	1.6	All	All	All
Operating System	Netbsd	Netbsd	1.6.1	All	All	All
Operating System	Netbsd	Netbsd	1.6.2	All	All	All
Operating System	Netbsd	Netbsd	2.0	All	All	All
Operating System	Netbsd	Netbsd	2.0.1	All	All	All
Operating System	Netbsd	Netbsd	2.0.2	All	All	All
Operating System	Netbsd	Netbsd	2.0.3	All	All	All
Operating System	Netbsd	Netbsd	2.1	All	All	All

cpe:2.3:o:netbsd:netbsd:1.6:*****:
cpe:2.3:o:netbsd:netbsd:1.6.1:*****:
cpe:2.3:o:netbsd:netbsd:1.6.2:*****:
cpe:2.3:o:netbsd:netbsd:2.0:*****:
cpe:2.3:o:netbsd:netbsd:2.0.1:*****:
cpe:2.3:o:netbsd:netbsd:2.0.2:*****:
cpe:2.3:o:netbsd:netbsd:2.0.3:*****:
cpe:2.3:o:netbsd:netbsd:2.1:*****:
cpe:2.3:o:netbsd:netbsd:1.6:*****:
cpe:2.3:o:netbsd:netbsd:1.6.1:*****:
cpe:2.3:o:netbsd:netbsd:1.6.2:*****:
cpe:2.3:o:netbsd:netbsd:2.0:*****:
cpe:2.3:o:netbsd:netbsd:2.0.1:*****:
cpe:2.3:o:netbsd:netbsd:2.0.2:*****:
cpe:2.3:o:netbsd:netbsd:2.0.3:*****:
cpe:2.3:o:netbsd:netbsd:2.1:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)