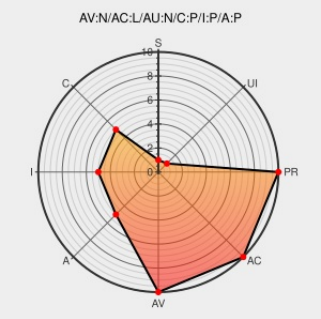
CVE-2005-4741

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 cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	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/exploitz/prdelka-vs-BSD-ptrace.tar.gz
No Description Provided	prdelka.blackart.org.uk Inactive Link Not Archived	MISC prdelka.blackart.org.uk/exploitz/prdelka-vs-BSD-ptrace.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

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→