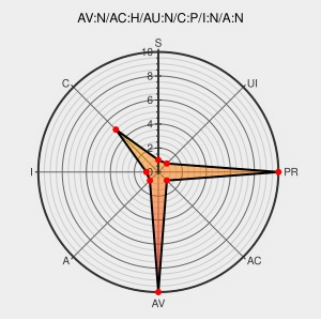
CVE-2006-1833

Published on: 04/19/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:01 PM UTC

CVE-2006-1833

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



Certain versions of Netbsd from Netbsd contain the following vulnerability:

Intel RNG Driver in NetBSD 1.6 through 3.0 may incorrectly detect the presence of the pchb interface, which will cause it to always generate the same random number, which allows remote attackers to more easily crack encryption keys generated from the interface.

CVE-2006-1833 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 2.6 - LOW

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF netbsd-intel-rng-security-bypass(25786)
NetBSD False Intel Hardware RNG Detection Predictable Random Number Generation Weakness	cve.report (archive) text/html	BID 17496
NetBSD Intel RNG Driver May Use a Constant Stream for Randomization - SecurityTracker	securitytracker.com text/html	SECTRACK 1015907
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24577
NetBSD False Intel Hardware RNG Detection Security Issue - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 19585

	ftp.netbsd.org text/plain	NETBSD NetBSD-SA2006-009

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	beta	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	3.0	All	All	All
Operating System	Netbsd	Netbsd	1.6	All	All	All
Operating System	Netbsd	Netbsd	1.6	beta	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

System						
Operating System	Netbsd	Netbsd	2.0.3	All	All	All
Operating System	Netbsd	Netbsd	2.1	All	All	All
Operating System	Netbsd	Netbsd	3.0	All	All	All

cpe:2.3:o:netbsd:netbsd:1.6:*:*:*:*:*:*:*:

cpe:2.3:o:netbsd:netbsd:1.6:beta:*:*:*:*:*:*:

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:3.0:*:*:*:*:*:*:*:

cpe:2.3:o:netbsd:netbsd:1.6:*:*:*:*:*:*:*:

cpe:2.3:o:netbsd:netbsd:1.6:beta:*:*:*:*:*:*:

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:3.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report