



CVE-2011-1920

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2011-1920
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-23 22:55:00 UTC
Updated	2017-08-17 01:34:00 UTC
Description	The make include files in NetBSD before 1.6.2, as used in pmake 1.111 and other products, allow local users to overwrite a

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ihji	Pmake	1.111	All	All	All
Application	Ihji	Pmake	1.111	All	All	All
Operating System	Netbsd	Netbsd	All	All	All	All
Operating System	Netbsd	Netbsd	1.0	All	All	All
Operating System	Netbsd	Netbsd	1.1	All	All	All
Operating System	Netbsd	Netbsd	1.2	All	All	All
Operating System	Netbsd	Netbsd	1.2.1	All	All	All
Operating System	Netbsd	Netbsd	1.3	All	All	All
Operating System	Netbsd	Netbsd	1.3.1	All	All	All
Operating System	Netbsd	Netbsd	1.3.2	All	All	All
Operating System	Netbsd	Netbsd	1.3.3	All	All	All
Operating System	Netbsd	Netbsd	1.4	All	All	All
Operating System	Netbsd	Netbsd	1.4.1	All	All	All
Operating System	Netbsd	Netbsd	1.4.2	All	All	All
Operating System	Netbsd	Netbsd	1.4.3	All	All	All
Operating System	Netbsd	Netbsd	1.5	All	All	All
Operating System	Netbsd	Netbsd	1.5.1	All	All	All

Operating System	Netbsd	Netbsd	1.5.2	All	All	All
Operating System	Netbsd	Netbsd	1.5.3	All	All	All
Operating System	Netbsd	Netbsd	1.6	All	All	All
Operating System	Netbsd	Netbsd	All	All	All	All
Operating System	Netbsd	Netbsd	1.0	All	All	All
Operating System	Netbsd	Netbsd	1.1	All	All	All
Operating System	Netbsd	Netbsd	1.2	All	All	All
Operating System	Netbsd	Netbsd	1.2.1	All	All	All
Operating System	Netbsd	Netbsd	1.3	All	All	All
Operating System	Netbsd	Netbsd	1.3.1	All	All	All
Operating System	Netbsd	Netbsd	1.3.2	All	All	All
Operating System	Netbsd	Netbsd	1.3.3	All	All	All
Operating System	Netbsd	Netbsd	1.4	All	All	All
Operating System	Netbsd	Netbsd	1.4.1	All	All	All
Operating System	Netbsd	Netbsd	1.4.2	All	All	All
Operating System	Netbsd	Netbsd	1.4.3	All	All	All
Operating System	Netbsd	Netbsd	1.5	All	All	All
Operating System	Netbsd	Netbsd	1.5.1	All	All	All
Operating System	Netbsd	Netbsd	1.5.2	All	All	All
Operating System	Netbsd	Netbsd	1.5.3	All	All	All
Operating System	Netbsd	Netbsd	1.6	All	All	All
Operating System	Netbsd	Netbsd	All	All	All	All

References

Reference	Source	Link
src/share/mk/bsd.lib.mk - diff - 1.240	CONFIRM	cvsweb.netbsd.org
Pmake Insecure Temporary File Creation Vulnerability	BID	www.securityfocus.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
src/share/mk/bsd.prog.mk - diff - 1.193	CONFIRM	cvsweb.netbsd.org
oss-security - CVE Request -- pmake -- Use of insecure temporary file for 'depend' target	MLIST	openwall.com
705090 – pmake: Use of insecure temporary file for 'depend' target	CONFIRM	bugzilla.redhat.com
oss-security - Re: CVE Request -- pmake -- Use of insecure temporary file for 'depend' target	MLIST	openwall.com
705100 – (CVE-2011-1920) CVE-2011-1920 mk-files: insecure temporary file usage	CONFIRM	bugzilla.redhat.com
#626673 - pmake: insecure temporary files - Debian Bug report logs	CONFIRM	bugs.debian.org
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)