



# CVE-2017-1000375

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

## Summary

<b>CVE</b>	CVE-2017-1000375
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-06-19 16:29:00 UTC
<b>Updated</b>	2017-08-12 01:29:00 UTC
<b>Description</b>	NetBSD maps the run-time link-editor ld.so directly below the stack region, even if ASLR is enabled, this allows attackers to

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Netbsd	Netbsd	All	All	All	All

## References

Reference	Source	Link	Tags
NetBSD CVE-2017-1000375 Arbitrary Code Execution Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory, VDB En
NetBSD - 'Stack Clash' (PoC) - NetBSD_x86 dos Exploit	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>	
<a href="http://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt">www.qualys.com/2017/06/19/stack-clash/stack-clash.txt</a>	MISC	<a href="http://www.qualys.com">www.qualys.com</a>	Exploit, Third Party Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#)**