CVE-2017-1000375

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-1000375
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-19 16:29:00 UTC
Updated	2017-08-12 01:29:00 UTC
Description	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	www.securityfocus.com	Third Party Advisory, VDB En
NetBSD - 'Stack Clash' (PoC) - NetBSD_x86 dos Exploit	EXPLOIT-DB	www.exploit-db.com	
www.qualys.com/2017/06/19/stack-clash/stack-clash.txt	MISC	www.qualys.com	Exploit, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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