



CVE-2020-24863

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

Summary

CVE	CVE-2020-24863
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-03 15:15:00 UTC
Updated	2020-09-11 14:03:00 UTC
Description	A memory corruption vulnerability was found in the kernel function kern_getfsstat in MidnightBSD before 1.2.7 and 1.3 thro

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	All	All	All	All
Application	Midnightbsd	Midnightbsd	All	All	All	All
Application	Midnightbsd	Midnightbsd	All	All	All	All
Application	Midnightbsd	Midnightbsd	All	All	All	All

References

Reference	Source	Link	Tags
www.freebsd.org/security/advisories/FreeBSD-EN-20:18.getfsstat.asc	CONFIRM	www.freebsd.org	Patch
www.midnightbsd.org/security/adv/MIDNIGHTBSD-SA-20:01.txt	CONFIRM	www.midnightbsd.org	Explo
src/vfs_syscalls.c at 1691c07ff4f27b97220a5d65e217341e477f4014 · MidnightBSD/src · GitHub	MISC	github.com	Explo
MidnightBSD Release Notes	MISC	www.midnightbsd.org	Relea
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

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](#)