



CVE-2018-17159

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

Summary

CVE	CVE-2018-17159
State	PUBLIC
Assigner	secteam@freebsd.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-04 15:29:00 UTC
Updated	2018-12-31 16:45:00 UTC
Description	In FreeBSD before 11.2-STABLE(r340854) and 11.2-RELEASE-p5, the NFS server lacks a bounds check in the READDIR

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Freebsd	Freebsd	11.2	p5	All	All
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Freebsd	Freebsd	11.2	p5	All	All

References

Reference	Source	Link
FreeBSD-SA-18:13	FREEBSD	security.freebsd.org
FreeBSD Network File System Multiple Security Vulnerabilities	BID	www.securityfocus.com
Secunia Advisories	MISC	secuniaresearch.flexerasoftware.com
FreeBSD NFS Server Code Flaws Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	www.securitytracker.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)