



CVE-2014-3219

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

Summary

CVE	CVE-2014-3219
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-09 22:29:00 UTC
Updated	2019-09-24 15:15:00 UTC
Description	fish before 2.1.1 allows local users to write to arbitrary files via a symlink attack on (1) /tmp/fishd.log.%s, (2) /tmp/.pac-cache

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Application	Fishshell	Fish	All	All	All	All
Application	Fishshell	Fish	All	All	All	All

References

Reference	Source	Link
Malformed Request	BID	v
[SECURITY] Fedora 19 Update: fish-2.1.0-9.fc19	FEDORA	li
[security-announce] openSUSE-SU-2019:2177-1: moderate: Security update f	SUSE	li
oss-security - Security release of fish shell 2.1.1	MLIST	v
Bug 1092091 – CVE-2014-2905 CVE-2014-2906 CVE-2014-2914 CVE-2014-3219 fish: multiple flaws fixed in upstream 2.1.1	CONFIRM	t
symlink attack in __fish_print_packages and spawning fishd (CVE-2014-3219) · Issue #1440 · fish-shell/fish-shell · GitHub	CONFIRM	g
[security-announce] openSUSE-SU-2019:2188-1: moderate: Security update f	SUSE	li
avoid symlink attacks in __fish_print_packages and spawning fishd · fish-shell/fish-shell@3225d7e · GitHub	CONFIRM	g
oss-security - Re: Upcoming security release of fish 2.1.1	MLIST	v
fish: Multiple vulnerabilities (GLSA 201412-49) — Gentoo security	GENTOO	s

CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
No vendor comments have been submitted for this CVE.	
Legacy QID Mappings	
690250 Free Berkeley Software Distribution (FreeBSD) Security Update for fish (6c083cf8-4830-11e4-ae2c-c80aa9043978)	

© [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](#)