



CVE-2022-20001

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

Summary

CVE	CVE-2022-20001
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-14 19:15:00 UTC
Updated	2023-11-07 03:42:00 UTC
Description	fish is a command line shell. fish version 3.1.0 through version 3.3.1 is vulnerable to arbitrary code execution. git repositories

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Fishshell	Fish	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 35 Update: fish-3.4.1-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fec
fish_git_prompt: be careful about git config by ridiculousfish · Pull Request #8589 · fish-shell/fish-shell · GitHub	MISC	github.c
Navigating to a compromised git repository may lead to arbitrary code exection · Advisory · fish-shell/fish-shell · GitHub	CONFIRM	github.c
Debian -- Security Information -- DSA-5234-1 fish	DEBIAN	www.de
[SECURITY] Fedora 35 Update: fish-3.4.1-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fec
[SECURITY] Fedora 36 Update: fish-3.4.1-1.fc36 - package-announce - Fedora Mailing-Lists		lists.fec
Fish: User-assisted execution of arbitrary code (GLSA 202309-10) — Gentoo security	GENTOO	security
[SECURITY] Fedora 36 Update: fish-3.4.1-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fec
Release fish 3.4.0 (released March 12, 2022) · fish-shell/fish-shell · GitHub	MISC	github.c
CVE Program record	CVE.ORG	www.cve

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[181067](#) Debian Security Update for fish (DSA 5234-1)

[182002](#) Debian Security Update for fish (CVE-2022-20001)

[282555](#) Fedora Security Update for fish (FEDORA-2022-cd2c5e0634)

[354349](#) Amazon Linux Security Advisory for fish : ALAS2022-2022-056

[502216](#) Alpine Linux Security Update for fish

[503923](#) Alpine Linux Security Update for fish

[691033](#) Free Berkeley Software Distribution (FreeBSD) Security Update for shells/fish (a3b10c9b-99d9-11ed-aa55-d05099fed512)

[710755](#) Gentoo Linux Fish User-assisted execution of arbitrary code Vulnerability (GLSA 202309-10)

[901092](#) Common Base Linux Mariner (CBL-Mariner) Security Update for fish (9070)

© [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](#)