# Fides: Privacy Request Identity Verification Bypass Vulnerability via Duplicate Detection

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-42303 |
| **State** | PUBLISHED |
| **Assigner** | GitHub_M |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-05-12 18:17:24 UTC |
| **Updated** | 2026-05-12 19:16:33 UTC |
| **Description** | Fides is an open-source privacy engineering platform. From 2.75.0 to before 2.83.2, Fides deployments that enable both su |

## Risk And Classification

**Primary CVSS:** v4.0 6.1 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:H/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-288 | CWE-306 | CWE-841 | CWE-288 CWE-288: Authentication Bypass Using an Alternate Path or Channel | CWE-306 CWE-306: Missing Authentication for Critical Function | CWE-841 CWE-841: Improper Enforcement of Behavioral Workflow

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | security-advisories@github.com | Secondary | 6.1 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/S |
| 4.0 | CNA | DECLARED | 6.1 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/S |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

High

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:H/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Ethyca | Fides | affected >= 2.75.0, < 2.83.2 | Not specified |

## References

| Reference | Source | Link |
|---|---|---|
| github.com/ethyca/fides/security/advisories/GHSA-qx5f-ghc2-7g5c | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | github.com |
| github.com/ethyca/fides/pull/7971 | security-advisories@github.com | github.com |
| github.com/ethyca/fides/releases/tag/2.83.2 | security-advisories@github.com | github.com |
| github.com/ethyca/fides/pull/7972 | security-advisories@github.com | github.com |
| github.com/ethyca/fides/commit/0e320b20934eb5af3a3d5127dba2691605d7ff37 | security-advisories@github.com | github.com |
| github.com/ethyca/fides/commit/e7a6527b0f9fdc9887b86a89bb5453e7421882dd | security-advisories@github.com | github.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.

**Free CVE JSON API** cve.report/api

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