# Frappe Framework 16.10.0 - Stored DOM XSS in Tag Pill Renderer

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-3673 |
| **State** | PUBLISHED |
| **Assigner** | Fluid Attacks |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-04-22 20:16:41 UTC |
| **Updated** | 2026-04-22 21:23:52 UTC |
| **Description** | An authenticated attacker can store a crafted tag value in _user_tags and trigger JavaScript execution when a victim opens |

## Risk And Classification

**Primary CVSS:** v4.0 4.6 MEDIUM from help@fluidattacks.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/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-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | help@fluidattacks.com | Secondary | 4.6 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E: |
| 4.0 | CNA | CVSS | 4.6 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

Active

Confidentiality

None

ntegrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/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 | Frappe | Frappe | affected 16.10.10 | Windows, MacOS, Linux |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| fluidattacks.com/es/advisories/silvio | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | fluidattacks.com | |
| github.com/frappe/frappe | help@fluidattacks.com | github.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

## Vendor Comments And Credit

Discovery Credit

**CNA:** Fluid Attacks' AI SAST Scanner (en)

**CNA:** Oscar Uribe (en)

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**