MightyNawaf / **CVE-2026-39087.md**

Created 2 weeks ago



# CVE-2026-39087: Server-Side Request Forgery (SSRF) in ntfy via Unanchored Web Push Endpoint Regex

## Affected Software

- **Product:** ntfy (https://github.com/binwiederhier/ntfy)
- **Affected Versions:** < 2.22.0
- **Fixed Version:** 2.22.0

## Vulnerability Type

Server-Side Request Forgery (SSRF) — CWE-918

## Description

The ntfy server used an unanchored regular expression to validate web push endpoint URLs. Because the regex pattern was not properly anchored, an attacker could craft a web push endpoint URL that matched the allow-list pattern while actually pointing to an arbitrary destination. This allowed the ntfy server to make HTTP requests to attacker-controlled or internal hosts on behalf of the server.

## Impact

An attacker could abuse the unanchored regex to bypass the web push endpoint allow-list and force the ntfy server to issue HTTP requests to internal or arbitrary external hosts. This could be used to probe internal network infrastructure, access internal services, or interact with cloud metadata endpoints.

## Remediation

The maintainer tightened the web push endpoint allow-list regex to enforce proper pattern anchoring, preventing SSRF via partial URL matching. The fix was released in ntfy v2.22.0.

## References

- Fix release: https://github.com/binwiederhier/ntfy/releases/tag/v2.22.0
- GitHub Security Advisory: GHSA-w9hq-5jg7-q4j7

## Credit

Reported by Nawaf Alshehri (@MightyNawaf)

## Timeline

- **2025-03-06:** Vulnerability reported to maintainer
- **2025-04-21:** Fix released in v2.22.0
- **2026-04-22:** CVE-2026-39087 requested from MITRE

**binwiederhier** commented last week • edited

I am the maintainer of ntfy.

The published CVE (https://www.cve.org/CVERecord?id=CVE-2026-39087) is **entirely inaccurate**. The description in this gist ("SSRF in ntfy via Unanchored Web Push Endpoint Regex") is correct. The published CVE talks about remote code execution in `parseActions`. Tis is inaccurate. There is no RCE in `parseActions`.

I've asked **@MightyNawaf** to correct this.