GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

3 September 2026

Advisory 250: fast-uri (npm) Authority Injection via Unvalidated Port Serialization (CVE-2026-84292).

Release Date: 2nd September 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations, System/Network administrators, and software development teams that build or operate Node.js applications depending on the fast-uri library, whether directly or transitively through widely-used packages such as ajv and the Fastify web framework. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-84292 is a high-severity vulnerability in fast-uri, a dependency-free URI parsing and serialization library for JavaScript/Node.js maintained under the OpenJS Foundation, and one of the most widely-used packages in the Node.js ecosystem.

What are the systems affected?

The following version(s) are affected:

- fast-uri before 2.4.6 - (Affected)
- fast-uri 3.0.0 up to (but not including) 3.1.7, and 4.0.0 up to (but not including) 4.1.4 – (Affected)

fast-uri 2.4.6, 3.1.7, and 4.1.4, and later on each respective branch - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Supply a crafted port value to an application using fast-uri**
    - An attacker supplies a URI or URI-like input containing a non-numeric “port” value (for example, one that begins with an “@” character) to an application that uses fast-uri to parse and then re-serialize that URI.
2. **Redirect the reconstructed authority to an attacker-controlled host**
    - Because fast-uri concatenates the unvalidated port value into the serialized output, the malicious port value injects an authority delimiter, demoting the application’s intended trusted host to a userinfo field and causing the reconstructed URI to actually point at an attacker-controlled host.

Attack vectors:

- A network-based, unauthenticated input against any application that uses an affected version of fast-uri (directly or transitively via ajv/Fastify) to parse and re-serialize URI data supplied by an untrusted party.
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:NSuccessful exploitation may allow attackers to:

- Cause an application to misinterpret an attacker-controlled host as the intended, trusted host after URI serialization, undermining any host-based allowlist, trust decision, or routing logic built on top of fast-uri’s output.
- Depending on how the affected application uses the resulting (incorrect) authority — for example, to make an internal request, issue a redirect, or authorize access to a downstream resource — potentially achieve server-side request forgery, an open redirect, or unauthorized access to internal systems the application did not intend to expose.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Upgrade fast-uri to version 2.4.6, 3.1.7, or 4.1.4 (whichever branch applies), where this vulnerability is fixed (GitHub Security Advisory GHSA-qw65-cvwx-89v3). Where fast-uri is a transitive dependency, upgrade the direct dependency (such as ajv or Fastify) to a version that bundles the fixed release.

2. Audit every application for a fast-uri dependency, direct or transitive, since this library is commonly pulled in indirectly and easy to overlook

3. Review any code that treats a fast-uri-serialized URI’s host or authority as trusted

4. Treat any unpatched, internet-facing application using fast-uri for untrusted URI input as a priority remediation target

5. Review logs for unexpected authority/host values

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-84292
2. https://github.com/fastify/fast-uri/security/advisories/GHSA-qw65-cvwx-89v3