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

8 July 2026

Advisory 153: @fastify/express & @fastify/middie Middleware Bypass Vulnerability.

Release Date: 06th July 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

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

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

1. **CVE-2026-6556** - @fastify/express Middleware Prefix Bypass - @fastify/express versions 4.0.6 and earlier only rewrite the plugin prefix for middleware mount paths when the path argument is a string. Non-string mount paths (arrays of paths and regular expressions) are left unprefixed inside prefixed plugin scopes, so middleware registered with those forms does not match the actual prefixed request path.

2. **CVE-2026-14198** - @fastify/middle Encoded Slash Bypass - @fastify/middie versions 9.1.0 through 9.3.2 decode the encoded slash (`%2F`) inside path parameter values before matching middleware paths, while Fastify's underlying router preserves the encoding during route lookup. The two layers disagree on the canonical request path, so the middleware fails to match a URL that the route handler does match.

3. **CVE-2026-14181** - @fastify/middie's standalone engine is vulnerable to Denial of Service via malformed percent-encoded paths. This is the same root defect class as CVE-2026-1418

(both are uncaught-exception DoS issues in the standalone engine's URL normalization), but tracked as a separate CVE ID — likely covering an overlapping or slightly different malformed-encoding trigger path.

What are the systems affected?

CVE-2026-6556 – Node.js applications using @fastify/express version 4.0.6 or earlier, specifically those with middleware registered inside prefixed plugin scopes using array or regex mount paths.

CVE-2026-14198 – Node.js applications using @fastify/middie versions 9.1.0–9.3.2 with middleware applied on parameterized paths for security enforcement.

CVE-2026-14181 - @fastify/middie versions 9.1.0 up to (but not including) 9.3.3 — same affected range as the other middie CVEs. Applications using the standalone engine API directly are affected; those using the Fastify plugin path are not, since Fastify's error handler catches the exception.

What does this mean?

CVE-2026-6556 - Applications that use path-scoped middleware for authentication, authorization, rate limiting, or auditing on routes inside a prefixed scope can be bypassed by sending a request to the prefixed route, because Fastify still matches the route but the middleware is skipped. This means an attacker can reach a route that appears protected — bypassing auth/rate-limiting checks entirely — simply by hitting the prefixed path directly.

CVE-2026-14198 - When middleware is used for authentication, authorization, rate limiting, or auditing on parameterized paths, an attacker can reach the protected handler by sending a single crafted URL with an encoded slash in the parameter position. The bypass is HTTP method agnostic and requires no authentication or special preconditions — making this trivially exploitable with a single request.

CVE-2026-14181 - A crafted request containing a malformed percent-encoded path segment causes the standalone engine's normalization step to throw an uncaught exception, crashing the Node.js process. No authentication is required, and per CISA's vulnerability scoring, this is rated as automatable — meaning it can be triggered reliably at scale/scripted, with a partial technical impact (single-process crash, not full system compromise).

Mitigation process

CERTVU recommends the following:

CVE-2026-6556

- **Patch:** Upgrade to @fastify/express 4.0.7.
- **Workaround (if immediate patching isn't possible):** Use string mount paths instead of arrays or regular expressions in prefixed plugins, or register one `use` call per path.

CVE-2026-14198

- **Patch:** Upgrade to @fastify/middie 9.3.3.
- **Workaround:** Avoid parameterized middleware paths for security decisions, or enforce authentication at the route handler or via a Fastify hook that runs after the router has resolved the request.

CVE-2026-14181

- **Patch:** Upgrade to @fastify/middie 9.3.3.

- **Workaround:** Migrate from the standalone engine API to the Fastify plugin path, where the framework error handler catches the exception before it can crash the process.

Reference

1. https://www.cisa.gov/news-events/bulletins/sb26-187
2. https://www.cve.org/CVERecord?id=CVE-2026-6556
3. https://www.cve.org/CVERecord?id=CVE-2026-14198
4. https://www.cve.org/CVERecord?id=CVE-2026-14181

.