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

23 April 2026

Advisory 138: Apache ActiveMQ Improper Input Validation Vulnerability (CVE-2026-34197).

Release Date: 16th April 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?

CVE-2026-34197 is a high-severity remote code execution (RCE) vulnerability (CVSS ~8.8) affecting Apache Tomcat.

The flaw is caused by improper input validation in HTTP request processing, specifically when handling certain malformed requests that can lead to memory corruption or unsafe object handling inside the server's request pipeline.

What are the systems affected?

The vulnerability affects;

- Apache Tomcat versions prior to the patched release (2026 security update cycle)

• Systems where Tomcat is deployed as:

- Standalone web server
- Backend application server for Java web applications
- Embedded server in enterprise applications

What does this mean?

Exploitation is remote and network-based**,** requiring only HTTP access.

Typical attack flow:

1. **Target identification**
   - Attackers scan for exposed Tomcat servers (port 8080/8443 or custom HTTP ports).
2. **Crafted HTTP request delivery**
   - A malicious request is sent containing specially structured headers or payload data.
3. **Triggering unsafe processing**
   - The server fails to properly validate or sanitize input during request parsing.
4. **Memory corruption / unsafe execution path**
   - Internal processing logic is manipulated, allowing execution of injected payloads.
5. **Remote code execution**
   - Attacker gains execution capability on the underlying server (often with the privileges of the Tomcat process).

Successful exploitation of this vulnerability may allow attackers to:

- Execute arbitrary code on the web server
- Deploy web shells or persistent backdoors
- Steal application data and credentials
- Modify web application content
- Pivot into internal enterprise networks
- Compromise cloud-hosted services

Because Tomcat often hosts critical business applications, compromise can lead to full application and data exposure.

Mitigation process

CERTVU recommends the following:

1. Apply Security Patches (Critical)

- Upgrade to the latest patched version of Apache Tomcat released in the 2026 security advisory cycle
- Ensure all instances (dev, test, production) are updated

2. Restrict Network Exposure

- Do not expose Tomcat management or admin interfaces to the internet

- Restrict access using:
  - VPN
  - IP allowlisting
  - Reverse proxy / WAF

3. Harden Configuration

- Disable unnecessary services (e.g., Manager/Host Manager if not required)
- Remove default or unused applications
- Enforce secure configuration of HTTP connectors

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-34197
3. https://www.herodevs.com/blog-posts/apache-tomcat-cve-round-up-10-vulnerabilities-patched-across-tomcat-9-10-and-11-april-2026

.