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

4 September 2026

Advisory 258: CAT (dianping) Admin Session Cookie Forgery (CVE-2026-85181).

Release Date: 3rd September 2026
Impact: 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, System/Network administrators, and DevOps/software engineering teams that deploy or operate CAT as a self-hosted application monitoring and diagnostics platform. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-85181 is a critical authentication bypass vulnerability in CAT, an open-source, self-hosted real-time application monitoring and diagnostics platform (18,900+ GitHub stars) originally built by Meituan-Dianping and offering clients for Java, C/C++, Node.js, Python, and Go. CAT uses Java's String.hashCode() as the sole integrity check on its session cookies, with no server-side secret key involved in generating or validating the checksum - meaning an attacker who understands this scheme can compute valid checksums offline and forge a session cookie without ever authenticating to the platform.

What are the systems affected?

The following version(s) are affected:

- CAT through 3.1.0, the current latest stable release - (Affected)

No fixed version has been published at the time of writing - see “Mitigation process” below

CAT is a self-hosted platform rather than a centrally-patched service, and — as with several recent CERTVU advisories — no fixed release exists for this issue at all at the time of writing. Organizations should not wait for a patch before acting: apply the network-level workarounds described below to every CAT deployment immediately, since the underlying application-level authentication mechanism cannot currently be trusted on its own.

What does this mean?

Typical attack flow:

1. **Forge a valid-looking admin session cookie offline**
    - Because CAT’s session cookie integrity check is a simple, un-keyed Java String.hashCode() computation, an attacker who understands the scheme can compute a matching checksum offline, without ever interacting with the target CAT deployment, and construct a cookie that CAT will treat as a valid session.
2. **Bypass IP-based access restrictions with a spoofed header**
    - The attacker sends the forged cookie to the CAT admin console together with a crafted X-Forwarded-For header claiming a trusted source IP address. On a deployment that trusts this client-supplied header without a reverse proxy correctly overwriting it, CAT’s IP validation is bypassed, and the attacker gains an unauthorized administrative session.

Attack vectors:

- A network-based, unauthenticated attack against any internet- or network-reachable CAT deployment whose admin console is exposed and does not have a reverse proxy correctly sanitising the X-Forwarded-For header.
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:N). CERTVU is not aware of confirmed active exploitation at the time of writing, but the technical mechanism is straightforward to reproduce offline, and no fixed version currently exists.

Successful exploitation may allow attackers to:

- Gain unauthorized administrative access to an affected CAT deployment without ever holding a legitimate credential.
- View, modify, or disrupt the monitoring, alerting, and performance-diagnostic data CAT collects across the applications it monitors — data that can itself reveal sensitive information about the architecture, dependencies, and behaviour of the systems behind it, providing a foothold for further reconnaissance or attack.

Mitigation process

CERTVU recommends the following:

1. Restrict network access to the CAT admin console immediately — no vendor patch is currently available

- Ensure CAT's admin console is reachable only from a trusted internal network or VPN, not directly from the internet, and place a reverse proxy in front of CAT that strips or overwrites any client-supplied X-Forwarded-For header before forwarding the request, so the header cannot be spoofed. This is a workaround, not a fix — the underlying weak cookie-integrity scheme remains present in the application.

2. Treat this as unpatched: CAT's maintainers had not released a fixed version or formal advisory at the time of writing
3. Audit the estate for CAT deployments
4. Monitor for a vendor fix and apply it once released
5. Review CAT access logs for anomalous admin sessions

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

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-85181
2. https://github.com/dianping/cat