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 259: Taipy Cross-Site WebSocket Hijacking via Wildcard socket.io CORS (CVE-2026-85183).

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 data science/development teams that build or operate web applications using the Taipy Python framework. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-85183 is a critical Cross-Site WebSocket Hijacking (CSWSH) vulnerability in Taipy, an open-source Python framework (19,200+ GitHub stars) published by Avaiga that lets data scientists and developers turn data and AI algorithms into production-ready web applications, including interactive dashboards and what-if scenario tools.

What are the systems affected?

The following version(s) are affected:

- Taipy through 4.1.1, the current latest stable release - (Affected)

What does this mean?

Typical attack flow:

1. **Lure a victim with an active Taipy session to an attacker-controlled webpage**
    - A victim who is currently logged into, or has an open browser session with, an affected Taipy application visits a webpage controlled by the attacker — for example via a phishing link or a malicious/compromised third-party site.
2. **Silently hijack the victim's WebSocket session across origins**
    - Because Taipy's socket.io server reflects any Origin header while accepting credentials, JavaScript running on the attacker's page can open a credentialed WebSocket connection to the victim's Taipy application in the background, without the victim noticing and without the CSRF protections that would normally block such a cross-origin request.

Attack vectors:

- A network-based attack against any internet- or network-reachable Taipy application, triggered when a victim with an active session visits an attacker-controlled webpage.
- No privileges beyond an existing victim session are required, but the attack does depend on the victim visiting a malicious page while that session is active (CVSS v4.0 UI:P / v3.1 UI:R). CERTVU is not aware of confirmed active exploitation at the time of writing, but the technique is well-documented (Cross-Site WebSocket Hijacking) and no fixed version currently exists.

Successful exploitation may allow attackers to:

- Read and modify the victim's session state within the affected Taipy application, including data displayed on dashboards and scenario-management screens.
- Invoke the application's own action callbacks on the victim's behalf — potentially triggering data changes, workflow actions, or file downloads that exfiltrate information — entirely without the CSRF protections that guard Taipy's regular HTTP endpoints.

Mitigation process

CERTVU recommends the following:

1. Restrict the socket.io CORS configuration immediately - no vendor patch is currently available

- Explicitly configure Taipy's socket.io server (cors_allowed_origins) to a specific, trusted origin list rather than the wildcard default, and disable credentialed cross-origin connections unless a named origin genuinely requires them. This is a workaround, not a fix - review the setting on every Taipy deployment, since the vulnerable default has been present since at least version 4.0.3.

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

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

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-85183
2. https://github.com/Avaiga/taipy