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 April 2026

Advisory 128: TrueConf Client Download of Code Without Integrity Check Vulnerability

Release Date: 02nd 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-2026-3502 is a high-severity vulnerability (CVSS ~8.1) affecting Atlassian Confluence deployments. The issue stems from improper input validation.

TrueConf Client contains a download of code without integrity check vulnerability. An attacker who is able to influence the update delivery path can substitute a tampered update payload. If the payload is executed or installed by the updater, this may result in arbitrary code execution in the context of the updating process or user.

What are the systems affected?

The following version affected;

- Affected at TrueConf Client versions 8.1.0 through 8.5.2

What does this mean?

If the payload is executed or installed by the updater, this may result in arbitrary code execution in the context of the updating process or user.

Attackers exploit the vulnerability remotely via crafted HTTP requests.

Successful exploitation of **CVE-2026-3502** may result in:

- Unauthorized access to sensitive system and application files
- Exposure of credentials, API keys, or configuration data
- Compromise of confidential organizational information
- Potential for remote code execution (when chained with other flaws)
- Lateral movement within enterprise environments

Given Confluence's role in storing internal documentation, this can lead to significant data leakage and operational risk.

Mitigation process

CERTVU recommends the following:

1. **Apply Security Updates Immediately**
    - Upgrade to the latest patched versions
    - Ensure all Confluence instances are updated across environments.
2. **Restrict external Access**
    - Limit exposure of Confluence to the internet
3. **Harden Application and system configuration**
    - Apply least privilege to application and file system accounts
    - Disable unused features or plugins
    - Restrict file system access permission

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-3502

.