

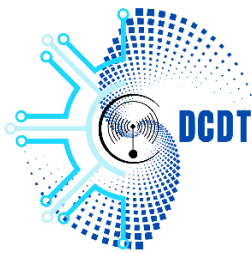
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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 157: Improper Input Validation — CVE-2026-48277, CVE-2026-48281,
CVE-2026-48315**

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?

ColdFusion doesn't adequately sanitize attacker-supplied input in certain request paths.

What are the systems affected?

ColdFusion 2025 (Update 9 and earlier), ColdFusion 2023 (Update 20 and earlier)

What does this mean?

How it's exploited:

- CVE-2026-48277 / CVE-2026-48281: A remote, unauthenticated attacker sends specially crafted input to a vulnerable component; the lack of sanitization allows that input to be processed in a way that leads to arbitrary code execution. No user interaction needed.

- CVE-2026-48315: Differs from the other two — despite being an "input validation" issue, exploitation requires a victim to open a malicious file, and success can lead to privilege escalation (described in some vendor writeups as enabling script injection that elevates the attacker's access within a session).

Mitigation process

CERTVU recommends the following:

- **Patch immediately:** Update to **ColdFusion 2025 Update 10** or **ColdFusion 2023 Update 21** as applicable. Given four CVEs in this batch are CVSS 10.0 and unauthenticated, treat this as urgent — Adobe itself has flagged that AI-assisted vulnerability research is compressing exploit timelines from days to hours.
- **Reduce exposure now, patch after:**
 - If file upload functionality is enabled anywhere in your ColdFusion deployment, verify authentication is enforced on the upload endpoint and consider disabling uploads until patched.
 - Restrict network access to ColdFusion admin/management interfaces to trusted internal networks or VPN.
 - Review outbound request capability from ColdFusion (relevant to the SSRF flaw) and restrict where the server itself can reach.
 - The 48315 case means user-awareness training (not opening untrusted ColdFusion-related files/links) is a relevant compensating control alongside patching.

Reference

1. <https://www.cisa.gov/news-events/bulletins/sb26-187>
2. <https://www.cve.org/CVERecord?id=CVE-2026-48277>
3. <https://www.cve.org/CVERecord?id=CVE-2026-48281>
4. <https://www.cve.org/CVERecord?id=CVE-2026-48315>

