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 159: Reflected XSS — CVE-2026-48307 Vulnerability

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?

A reflected cross-site scripting flaw.

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:

Attacker crafts a malicious link; **requires a victim to click it**. Successful exploitation injects scripts into the page in the victim's session context, which can escalate to arbitrary code execution in the context of the current user — more severe than a typical reflected XSS because of that RCE chain.

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.

Reference

1. https://www.cisa.gov/news-events/bulletins/sb26-187
2. https://www.cve.org/CVERecord?id=CVE-2026-48307

.