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 158: Path Traversal — CVE-2026-48282, CVE-2026-48313

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?

Improper limitation of pathnames allows access outside the intended directory scope.

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-2026-48282: An unauthenticated attacker manipulates path input to write files outside the restricted directory, leading to arbitrary code execution — described by watchTowr Labs as effectively an arbitrary file write, and the same fix reportedly also closed related (unassigned) issues around arbitrary file move/delete and directory creation/listing.

- CVE-2026-48313: A path traversal issue limited to arbitrary file system read (and limited write) — an attacker can access sensitive files/directories outside the intended scope, described as an arbitrary file read. No code execution on its own, but valuable for reconnaissance or credential/config theft that enables further attacks.

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-2026-48282
3. https://www.cve.org/CVERecord?id=CVE-2026-48313

.