

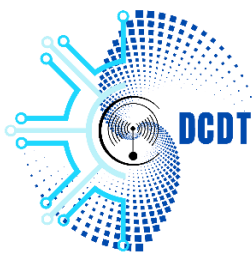
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

9 October 2026

Advisory 348: ProFTPD mod_copy Unauthenticated Arbitrary File Read and Write Vulnerability - Actively Exploited (CVE-2015-3306).

Release Date: 8th October 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 and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2015-3306 is an improper access control vulnerability (CWE-284) in the mod_copy module of ProFTPD. The SITE CPCR and SITE CPTO commands, which copy files on the server, can be used by an unauthenticated remote attacker to read and write arbitrary files that the FTP service account can reach. In practice an attacker can copy a PHP or script payload into a web-accessible directory and run it, which turns the file copy flaw into remote code execution. It carries a CVSS v2 score of 10.0; NVD has not published a CVSS v3 score.

What are the systems affected?

The following ProFTPD versions are affected where the mod_copy module is loaded:

- ProFTPD 1.3.5 before 1.3.5a (NVD lists version 1.3.5); mod_copy must be enabled in the server configuration

Not affected / patched version:

- ProFTPD 1.3.5a, 1.3.6rc1 or any later release, including the current stable ProFTPD releases. Linux distributions also published backported fixes (for example Debian DSA-3263), so check the vendor package changelog

What does this mean?

Successful exploitation may allow attackers to:

- Copy any file readable by the FTP service to another location, including configuration files and credentials, without logging in
- Write attacker-controlled files into web roots or other paths the service can write to, and run them as code
- Gain a foothold on a server, often a web or file-transfer host, and use it for malware hosting, data theft or movement into the internal network

Mitigation process

CERTVU recommends the following:

1. Upgrade ProFTPD

Upgrade to ProFTPD 1.3.5a or later, preferably the current stable release, and install distribution security updates.

2. Disable mod_copy if it is not needed

3. Reduce FTP exposure

4. Limit what the service can write

5. Hunt for compromise

Search FTP logs for SITE CPFR and SITE CPTO commands from unauthenticated sessions, check web roots for unexpected PHP or script files, and report suspected compromise to CERTVU.

Reference

1. <https://nvd.nist.gov/vuln/detail/CVE-2015-3306>
2. <https://www.exploit-db.com/exploits/49908>
3. <https://dailycve.com/proftpd-arbitrary-file-read-and-write-cve-2015-3306-critical-dc-oct2026-2939/>
4. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>