

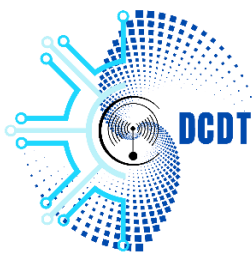
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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 349: ONLYOFFICE Document Server Path Traversal Remote Code Execution Vulnerability - Actively Exploited (CVE-2021-3199).

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-2021-3199 is a path traversal vulnerability (CWE-22) in the /upload endpoint of ONLYOFFICE Document Server, the document editing server used by ONLYOFFICE Docs and by products that integrate it. A ../ sequence in an image upload parameter lets an unauthenticated attacker write files outside the intended directory when JWT is in use, which can lead to remote code execution. CVSS v3.1 score: 9.8 (Critical); NVD also lists CVSS v2 7.5.

What are the systems affected?

The following ONLYOFFICE product versions are affected:

- ONLYOFFICE Document Server versions before 5.6.3, including ONLYOFFICE Docs and platforms that embed an unpatched Document Server

Not affected / patched version:

- ONLYOFFICE Document Server 5.6.3 or later. Current supported releases are strongly recommended, because 5.6.3 is an old release

What does this mean?

Successful exploitation may allow attackers to:

- Write files to arbitrary locations on the Document Server and run code on it, without credentials
- Take over the server and access documents it processes, which may include sensitive files from connected platforms such as file sharing, mail and collaboration suites
- Use the compromised server as a foothold into the internal network

Mitigation process

CERTVU recommends the following:

1. Upgrade immediately

Upgrade ONLYOFFICE Document Server to the latest supported release, and at minimum to 5.6.3 or later. Check any product that bundles Document Server, such as collaboration or mail suites, and update it too.

2. Find all instances

3. Restrict exposure

4. Check for compromise

5. Treat this as top priority

This vulnerability is listed in the CISA Known Exploited Vulnerabilities (KEV) catalog with a federal remediation deadline of 11 October 2026. Rotate the JWT secret and credentials if compromise is suspected, and report to CERTVU.

Reference

1. <https://nvd.nist.gov/vuln/detail/CVE-2021-3199>
2. <https://app.opencve.io/cve/CVE-2021-3199>
3. <https://cve-security.com/cve/cve-2021-3199>
4. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>