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

28 August 2026

Advisory 204: CVE-2023-49105_ownCloud Server WebDAV API Authentication Bypass Vulnerability

Release Date: 27th August 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

Any organisation operating a self-hosted ownCloud Server for file storage, sharing or synchronisation. Self-hosted file sharing platforms are commonly adopted where commercial cloud storage is costly or bandwidth-constrained, and where data is required to remain within the country. In Vanuatu this is most likely to apply to government agencies, non-government organisations and development partners, tertiary and technical institutions, and small and medium businesses.

What is it?

CVE-2023-49105 is an authentication bypass vulnerability (CWE-287) in the WebDAV API of ownCloud Server, carrying a CVSS Base Score of 9.8. It allows a remote, unauthenticated attacker to access, modify or delete any file belonging to a user whose username the attacker knows.

The flaw lies in the validation of pre-signed URLs. Pre-signed URLs are intended to grant temporary access to a file without the recipient supplying credentials, and their integrity depends on a signing key held by the file owner. Where a user has no signing key configured, the vulnerable code does not reject the request. Instead it proceeds with an empty key, with the result that an attacker can generate valid pre-signed URLs for arbitrary file operations on that user's files.

CERTVU emphasises that having no signing key configured is the default state. This is not an unusual or misconfigured deployment; a default installation is a vulnerable installation.

What are the systems affected?

- ownCloud Server (owncloud/core) versions 10.6.0 up to and including 10.13.0 - (Affected)

- ownCloud Server 10.13.3 and later - (Not affected, patched)

ownCloud advises that all instances below version 10.13.3 should be updated.

The running version is shown on the ownCloud administration page, and can also be read from the server configuration file:

```
grep version /path/to/owncloud/config/config.php
```

What does this mean?

The only prerequisite for exploitation is knowledge of a valid username. In most organisations usernames follow a predictable convention based on staff names, are visible in email addresses, or can be enumerated, so this is a low barrier rather than a meaningful control.

The consequence affects all three properties of the data at once. An attacker can read files, giving loss of confidentiality; modify them, giving loss of integrity; and delete them, giving loss of availability. There is no partial exposure here in which data is readable but safe from alteration.

A file sharing platform typically holds the material an organisation considers most sensitive, including personnel records, financial documents, case files, scanned identity documents, contracts and correspondence. Where such a platform holds personal information, unauthorised access to it may also constitute a reportable matter under the Data Protection and Privacy Act No. 13 of 2024, and organisations should consider their obligations accordingly.

The ability to modify and delete files introduces two further risks that are sometimes overlooked. An attacker able to write to a synchronised folder can distribute malicious files to every user and device that synchronises with it. An attacker able to delete files can conduct a destructive or extortion-based attack against an organisation's primary document store.

Mitigation process

CERTVU recommends the following:

1. Verify the Running Version

Check the version of every ownCloud Server instance, including any deployed by a department or project team outside central IT. Do not rely on a recollection of action taken in 2023; confirm the version currently running.

2. Upgrade to 10.13.3 or Later

Upgrade all affected instances to ownCloud Server 10.13.3 or later. Deleting files or disabling individual applications does not remediate this vulnerability; a core server upgrade is required. Given the CVSS score of 9.8, the unauthenticated nature of the flaw and the availability of public exploit code, CERTVU recommends treating this as an emergency change.

Other mitigating options include;

- Restrict Internet Exposure
- Assume Compromise Where the Instance Was Exposed
- Verify File Integrity and Restore Points
- Consider Data Protection Obligations

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2023-49105
2. https://owncloud.com/blogs/immediate-action-required-critical-security-updates-for-owncloud/
3. https://nvd.nist.gov/vuln/detail/CVE-2023-49105
4. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
5. https://cwe.mitre.org/data/definitions/287.html