National Cyber Security Centre

2311280107-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

ownCloud - Multiple Critical Vulnerabilities

Tuesday 28th November, 2023

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

ownCloud has released a software update which addresses a number of critical vulnerabilities, CVE-2023-49103, CVE-2023-49105, and CVE-2023-49104. If exploited, these vulnerabilities could allow for sensitive information disclosure and authentication bypass.

ownClouds security advisories can be found here:

- CVE-2023-49103 - Sensitive credential and configuration disclosure
- CVE-2023-49104 - Subdomain Validation Bypass
- CVE-2023-49105 - WebDAV API Authentication Bypass

The vulnerabilities have Exploit Prediction Scoring System (EPSS) scores of:

- CVE-2023-49103: 81%
- CVE-2023-49104: 7%
- CVE-2023-49105: 7%

Products Affected

The vulnerabilities affect different ownCloud components and applications.

- CVE-2023-49103 affects: graphapi application versions 0.2.0 – 0.3.0
- CVE-2023-49104 affects: oauth2 application versions prior to 0.6.1
- CVE-2023-49105 affects: ownCloud core versions 10.6.0 – 10.13.0

Impact

- Exploitation of CVE-2023-49103 could disclose the configuration of the PHP environment. In a containerized ownCloud deployment, additional sensitive information such as the ownCloud admin password, mail server credentials, and license key could be disclosed.
- Exploitation of CVE-2023-49104 could allow an attacker to redirect callbacks to a TLD owned by the attacker.
- Exploitation of CVE-2023-49105 could allow an attacker with knowledge of the victim user name to access, modify or delete any file without authentication.

The NCSC is aware that CVE-2023-49103 is under active exploitation at the time of writing.

Recommendations

The NCSC strongly advises affected organisations to review the latest ownCloud and related applications' release notes and install the relevant updates.

Additional recommendations and mitigation's for each CVE can be found in the respective links below:

- CVE-2023-49103 - Sensitive credential and configuration disclosure
- CVE-2023-49104 - Subdomain Validation Bypass
- CVE-2023-49105 - WebDAV API Authentication Bypass

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie