aDvens

Security for the greater good

Newscast

Critical vulnerability in OwnCloud

2023-11-27 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

CVE-2023-49103 2
Type of vulnerability 2
Risks 2
Severity (base score CVSS 3.1) 3
Impacted Products 3
Recommendations 3
Proof of concept 3
SOURCES 4

CVE-2023-49103

On 21 november 2023, OwnCloud published a security advisory about a new critical vulnerability(CVE-2023-49103) in their solution.

Two other vulnerabilities were listed in this security advisory : CVE-2023-49104 and CVE-2023-49105.

OwnCloud is an open-source solution for setting up your own file storage, sharing and synchronisation server.

The flaw impacts the *graphapi* application, which relies on a third-party library to generate a URL.

By accessing this URL, an attacker can retrieve PHP environment configuration information (phpinfo), including the administrator password and credentials for the email server configured in ownCloud.

While there is no evidence of exploitation of this vulnerability yet, a proof of concept (POC) is available. Approximately 2000 servers, accessible both on the internet and locally in France, are running ownCloud services.

Type of vulnerability

- **CWE-200**: Exposure of Sensitive Information to an Unauthorized Actor

Risks

- Data privacy breach
- Data integrity breach
- Security policy bypass

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

- OwnCloud graphapi library versions 0.2.x
- OwnCloud graphapi library versions 0.3.x
- Docker containers built before February 2023 are not vulnerable to the disclosure of credentials.

Recommendations

The provider recommends deleting the *GetPhpInfo* file located in owncloud/apps/graphapi/vendor/microsoft/microsoft-graph/tests/.

Further information is available in the editor's security advisory.

Proof of concept

A proof of concept is available in open source.

Sources

- https://owncloud.com/security-advisories/disclosure-of-sensitive-credentials-and-configuration-in-containerized-deployments/
- https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0970/