Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

ownCloud Critical Vulnerability is under active exploitation

Date of Publication	Admiralty Code	TA Number
November 30, 2023	A1	TA2023482

Summary

First Seen: November 25, 2023
Affected Product: ownCloud
Impact: Hackers are actively exploiting a critical vulnerability (CVE-2023-49103) in ownCloud, a popular open-source file-sharing solution, exposing sensitive data in containerized deployments. Administrators are urged to promptly apply recommended fixes, including disabling the 'phpinfo' function and changing exposed credentials.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-49103	ownCloud graphapi app Information Disclosure Vulnerability	ownCloud	✗	✓	✓
CVE-2023-49104	ownCloud oauth2 Subdomain Validation Bypass Vulnerability	ownCloud	✗	✗	✓
CVE-2023-49105	ownCloud core improper authentication Vulnerability	ownCloud	✗	✗	✓

Vulnerability Details

#1

A critical vulnerability, CVE-2023-49103, has been identified in ownCloud, an open-source file server. This vulnerability allows attackers to access admin passwords, mail server credentials, and license keys. Exploitation attempts have been observed, prompting concerns in the cybersecurity community. The vulnerability affects ownCloud versions 0.2.0 to 0.3.0, particularly within the "graphapi" app, exposing sensitive information through a third-party library (GetPhpInfo.php). The severity of the situation is emphasized by its maximum CVSS score of 10.

#2

ownCloud developers released security bulletins on November 21, urging administrators to apply mitigations. Threat tracking firms have observed active exploitation of the vulnerability since November 25, 2023. Over 11,000 IPs are currently accessible, with scans originating from various locations, suggesting coordinated efforts.

#3

The advisory also addresses two additional critical vulnerabilities, CVE-2023-49104 and CVE-2023-49105, with recommendations for their respective mitigations. The first involves subdomain validation bypass, and the second is an authentication bypass vulnerability affecting WebDAV API in specific ownCloud versions.

#4

Mitigation methods recommended by ownCloud involve specific actions, including deleting a directory and changing compromised secrets. Notably, disabling the "graphapi" app is not considered an effective resolution, it affects both containerized and non-containerized environments. Only Docker containers created before February 2023 are resistant to the credential disclosure problem. Administrators are advised to take immediate action to address the risk posed by this vulnerability.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-49103	ownCloud graphapi 0.2.0 – 0.3.0	cpe:2.3:a:owncloud:graphapi:*:*:*:*:*:*:*	CWE-200
CVE-2023-49104	ownCloud oauth2 < 0.6.1	cpe:2.3:a:owncloud:oauth2:*:*:*:*:*:*:*	CWE-284
CVE-2023-49105	ownCloud Server: 10.6.0 - 10.13.0	cpe:2.3:a:owncloud:core:*:*:*:*:*:*:*	CWE-665

Recommendations

Immediate Patching and Update: Organizations using ownCloud should promptly update their installations to the latest version, which includes patches for CVE-2023-49103 and other disclosed vulnerabilities. Regularly check for software updates and security patches provided by ownCloud to address emerging threats.

Delete Specific File: Locate and delete the file 'owncloud/apps/graphapi/vendor/microsoft/Microsoftgraph/tests/GetPhpInfo.php.' This file is identified as the source of the vulnerability and should be removed to prevent further exploitation.

Disable 'phpinfo' Function in Docker Containers: In Docker containers, disable the 'phpinfo' function to prevent the execution of phpinfo() through the ownCloud 'graphapi' app. This step is crucial for securing sensitive data within containerized deployments.

Update Credentials: Change potentially exposed secrets, including but not limited to the ownCloud admin password, mail server credentials, database credentials, and Object-Store/S3 access keys. This is essential to safeguard against unauthorized access resulting from the disclosed credentials.

Potential MITRE ATT&CK TTPs

TA0006 Credential Access	TA0043 Reconnaissance	TA0040 Impact	TA0042 Resource Development
T1589.001 Credentials	T1589 Gather Victim Identity Information	T1588.005 Exploits	T1588 Obtain Capabilities
T1588.006 Vulnerabilities			

Patch Links

https://marketplace.owncloud.com/apps/graphapi

https://marketplace.owncloud.com/apps/oauth2

https://owncloud.com/download-server

References

https://isc.sans.edu/diary/Scans+for+ownCloud+Vulnerability+CVE202349103/30432

https://www.helpnetsecurity.com/2023/11/28/cve-2023-49103/

https://owncloud.com/security-advisories/disclosure-of-sensitive-credentials-and-configuration-in-containerized-deployments/

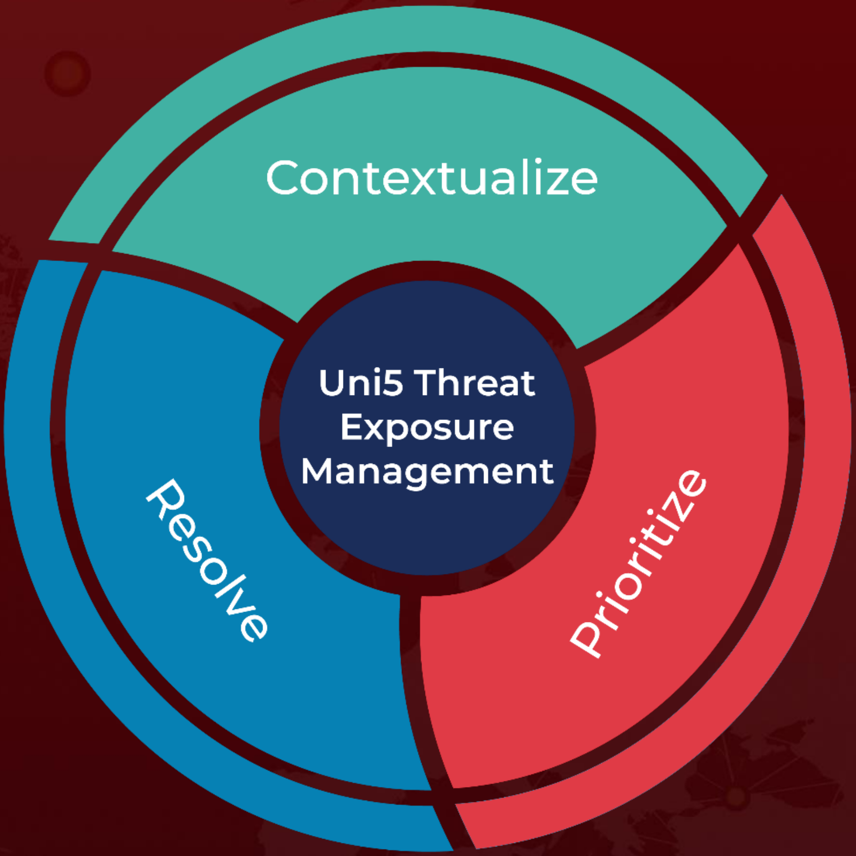
https://owncloud.com/security-advisories/subdomain-validation-bypass/

https://owncloud.com/security-advisories/webdav-api-authentication-bypass-using-pre-signed-urls/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 30, 2023 • 4:30 AM

More at www.hivepro.com