HC3: White Paper

December 5, 2023 TLP:CLEAR Report: 202312051700

ownCloud Vulnerability Under Active Attack

Executive Summary

The ownCloud platform allows organizations to store, synchronize, and share files and other content, as well as collaborate and consolidate work processes. This platform is known to be deployed across the U.S. health sector, among other industries. The nature of this platform provides cyber-attackers with a target that can potentially provide access to sensitive health information, as well as a staging point for further attacks. Three vulnerabilities were recently identified in certain versions of ownCloud, the most egregious of which is known to be under active attack. HC3 recommends healthcare organizations running ownCloud identify vulnerable instances and prioritize implementation of the mitigation steps in this document.

Platform Overview

The ownCloud platform is described on its website as an "open-source file sync, share and content collaboration software that lets teams work on data easily from anywhere, on any device." The company reports 500 enterprise customers and 200 million users worldwide. It serves the health sector, among other industries, where it has noted that it "enables users to collaborate while retaining digital sovereignty, empowering them to easily edit, share, and access files regardless of device or location. Tailored open–source solutions without backdoors or vendor lock-ins." Its stated capabilities include HIPAA compliance, securely storing and sharing sensitive patient data, and frictionless collaboration among medical professionals, among other features. A capabilities document can be found here. The nature of this platform is such that it needs to be integrated into the information infrastructure of a customer organization to function, which provides attackers with a target that can potentially provide access to sensitive information, as well as a staging point for further attacks.

Vulnerabilities

On November 21, 2023, ownCloud released three security advisories applicable to the ownCloud platform:

1. A credential theft and configuration in containerized deployments vulnerability, tracked as CVE-2023-49103 and assigned a CVSS severity rating of 10.0 out of 10.0. This vulnerability impacts graphapi 0.2.0 through 0.3.0 and is related to the app's dependency on a third-party library that exposes PHP environment details (phpinfo) through a URL, which includes the webserver's environment variables, and in containerized deployments, the ownCloud admin password, mail server credentials, and license key.
2. A WebDAV API authentication bypass vulnerability tracked as CVE-2023-49105 and assigned a CVSS security rating of 9.8 out of 10.0. This impacts ownCloud core library versions 10.6.0 to 10.13.0 and allows for an attacker to access, modify, or delete any file without authentication if they have a username and they leverage a pre-signed URL (no signing-key has been configured).
3. A subdomain validation bypass vulnerability tracked as CVE-2023-49104 and assigned a CVSS security rating of 9 out of 10.0. This impacts all versions of the oauth2 library prior to version 0.6.1. This vulnerability allows for an attacker to input a crafted redirect URL that can bypass the oauth2 app validation code, which can allow for redirection of callbacks to a malicious domain.

Active Exploitation

On November 27, 2023, Greynoise published research on the active exploitation of the first (CVE-2023-49103) of the above three vulnerabilities. They observed this exploitation originating from 32 unique IP

addresses beginning on November 25, 2023 and continuing for several days. (See **Figure 1** below.)

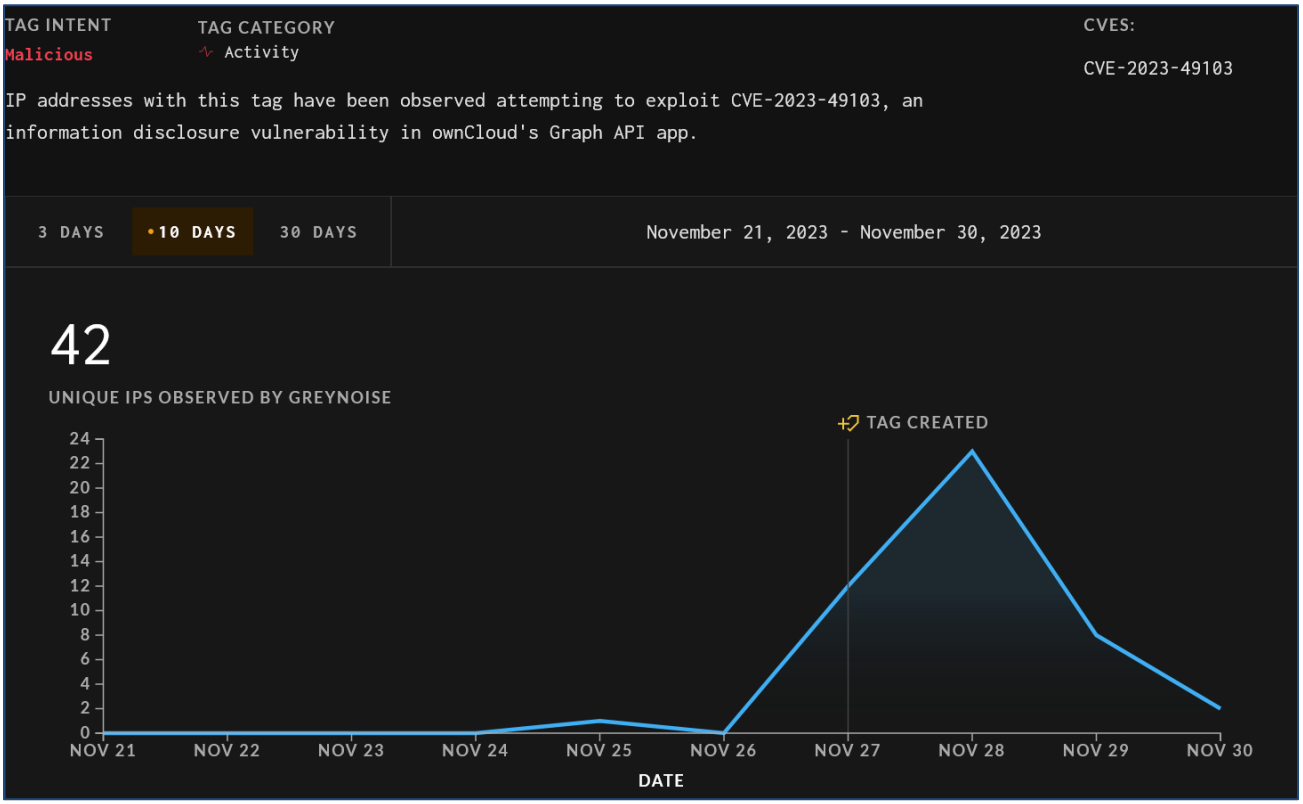

Figure 1:

Exploitation of CVE-2023-49103 in late November 2023. *(Source: Greynoise)*

Shadowserver Foundation analysts also observed exploitation of CVE-2023-49103, and identified over 10,000 vulnerable instances around the world, including 1,400 in the United States. (See **Figure 2** below.)

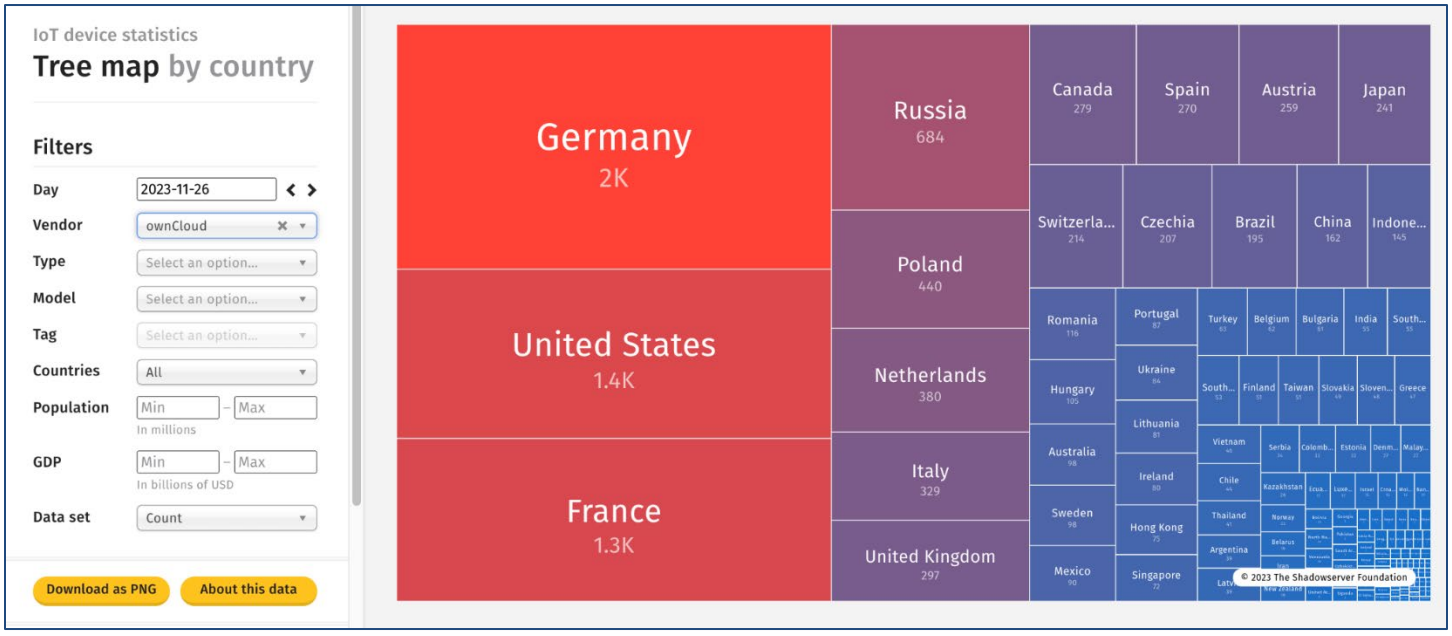

Figure 2: Global instances of vulnerable ownCloud instances. *(Source: Shadowserver Foundation)*

Countermeasures and Mitigations

The recommended fixes for the three vulnerabilities are as follows:

The first vulnerability (CVE-2023-49103) is the one that is being actively exploited and should be treated with the highest priority. In the recommended remediation steps, they emphasize that disabling the graphapi app does not eliminate the vulnerability and that an organization should delete the "owncloud/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php" file, disable the 'phpinfo' function in Docker containers, and change potentially exposed secrets, such as the credentials for ownCloud administration, the mail server, the database, and the Object-Store/S3 access key.

They also note that Docker-Containers from before February 2023 are not vulnerable to the credential disclosure.

The published solution for the second vulnerability is to deny the use of pre-signed URLs if no signing key is configured for the owner of the files.

The recommended mitigation for the third vulnerability is to harden the validation code in the Oauth2 app. They also note that a temporary workaround shared in the bulletin is to disable the "Allow Subdomains" option.

References

CVE-2023-49103: ownCloud Critical Vulnerability Quickly Exploited in the Wild
https://www.greynoise.io/blog/cve-2023-49103-owncloud-critical-vulnerability-quickly-exploited-in-the-wild

Critical bug in ownCloud file sharing app exposes admin passwords
https://www.bleepingcomputer.com/news/security/critical-bug-in-owncloud-file-sharing-app-exposes-admin-passwords/

Hackers start exploiting critical ownCloud flaw, patch now
https://www.bleepingcomputer.com/news/security/hackers-start-exploiting-critical-owncloud-flaw-patch-now/

ownCloud for Healthcare
https://oc.owncloud.com/rs/038-KRL-592/images/Whitepaper_ownCloud_for_Healthcare_EN.pdf

ownCloud: Benefit from the digital transformation in Healthcare
https://owncloud.com/industry-solutions/digitalization-in-healthcare/

ownCloud: Subdomain Validation Bypass
https://owncloud.com/security-advisories/subdomain-validation-bypass/

ownCloud: WebDAV Api Authentication Bypass using Pre-Signed URLs
https://owncloud.com/security-advisories/webdav-api-authentication-bypass-using-pre-signed-urls/

ownCloud: Disclosure of sensitive credentials and configuration in containerized deployments

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

Shadowserver Foundation on Mastodon, Posting from November 27, 2023 at 13:35
https://infosec.exchange/@shadowserver/111483954554586644

NIST CVE-2023-49103 Detail
https://nvd.nist.gov/vuln/detail/CVE-2023-49103

NIST CVE-2023-49104 Detail
https://nvd.nist.gov/vuln/detail/CVE-2023-49104

NIST CVE-2023-49105 Detail
https://nvd.nist.gov/vuln/detail/CVE-2023-49105

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback