Overall rating: Critical

BRITISH
COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that ownCloud published security advisories to address vulnerabilities in multiple products. Included were critical updates for the following:

- ownCloud graphapi – version 0.20 to 0.30
- ownCloud oauth2 – prior to version 0.6.1
- ownCloud core – version 10.6.0 to 10.13.0

The Cyber Centre has received reports that CVE-2023-49103 has been exploited.

Technical Details

An issue was discovered in ownCloud owncloud/graphapi 0.2.x before 0.2.1 and 0.3.x before 0.3.1. The graphapi app relies on a third-party GetPhpInfo.php library that provides a URL. When this URL is accessed, it reveals the configuration details of the PHP environment (phpinfo). This information includes all the environment variables of the webserver. In containerized deployments, these environment variables may include sensitive data such as the ownCloud admin password, mail server credentials, and license key. Simply disabling the graphapi app does not eliminate the vulnerability. Additionally, phpinfo exposes various other potentially sensitive configuration details that could be exploited by an attacker to gather information about the system. Therefore, even if ownCloud is not running in a containerized environment, this vulnerability should still be a cause for concern. Note that Docker containers from before February 2023 are not vulnerable to credential disclosure.

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.

- Notify business owner(s) as required.

- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-49103

- [ownCloud Security Advisory – graphapi](#)
- [ownCloud Security Advisory – oauth2](#)
- [ownCloud Security Advisory – core](#)
- [ownCloud Security Advisories](#)