

BOLETÍN DE ALERTA

Boletín 2023-52

Fecha de Publicación: 24/11/2023

Tema: Vulnerabilidad de divulgación de credenciales a través de la librería graphapi en ownCloud.

Productos afectados:

- Versiones 0.2.0 - 0.3.0 de la aplicación "graphapi" de ownCloud.

Descripción:

La aplicación "graphapi" de ownCloud utiliza una biblioteca de terceros que podría revelar información confidencial del entorno PHP (phpinfo) cuando se accede a una URL específica. Esta información incluye variables de entorno del servidor web, que pueden contener datos sensibles como contraseñas de administrador de ownCloud, credenciales del servidor de correo y clave de licencia. Incluso si ownCloud no se ejecuta en un entorno basado en contenedores. La vulnerabilidad fue identificada como CVE-2023-49103 con una puntuación asignada de 10 CVSS.

Impacto:

Un actor malicioso podría aprovechar esta vulnerabilidad para acceder a credenciales de administrador del sistema afectado.

Solución:

El fabricante recomienda tomar las siguientes medidas para mitigar esta vulnerabilidad:

- Eliminar el archivo owncloud/apps/graphapi/vendor/microsoft/microsoft/microsoft-graph/tests/GetPhpInfo.php.
- Desactivar la función phpinfo en los contenedores Docker.
- Cambiar las siguientes contraseñas y credenciales:

-Contraseña de administrador de ownCloud.

-Credenciales del servidor de correo.

-Credenciales de la base de datos.

-Clave de acceso a Object-Store/S3.

Se espera que futuras versiones de ownCloud incluyan medidas adicionales para fortalecer la seguridad y mitigar vulnerabilidades similares.

Información adicional:

- <https://owncloud.com/security-advisories/disclosure-of-sensitive-credentials-and-configuration-in-containerized-deployments/>
- <https://nvd.nist.gov/vuln/detail/CVE-2023-49103>
- <https://owncloud.org/security>