Los responsables del software de intercambio de archivos de código abierto ownCloud han alertado sobre tres vulnerabilidades de seguridad críticas que podrían ser aprovechadas para revelar información confidencial y modificar archivos.

Aquí hay una breve descripción de las vulnerabilidades:

1. Revelación de credenciales y configuración sensible en despliegues contenerizados que afectan a las versiones de graphapi desde 0.2.0 hasta 0.3.0 (puntuación CVSS: 10.0).
2. Bypass de autenticación de la API WebDAV mediante el uso de URL prefirmadas que afecta a las versiones principales desde 10.6.0 hasta 10.13.0 (puntuación CVSS: 9.8).
3. Bypass de validación de subdominios que afecta a oauth2 antes de la versión 0.6.1 (puntuación CVSS: 9.0).

> *«En relación con la primera vulnerabilidad, la aplicación 'graphapi' depende de una biblioteca de terceros que suministra una URL. Al acceder a esta URL, se revelan los detalles de configuración del entorno PHP (phpinfo)»,* declaró la compañía.

> *«Esta información incluye todas las variables de entorno del servidor web. En despliegues contenerizados, estas variables de entorno pueden contener datos confidenciales como la contraseña del administrador de ownCloud, las credenciales del servidor de correo y la clave de licencia».*

Como solución, ownCloud recomienda eliminar el archivo *«owncloud/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php»* y deshabilitar la función 'phpinfo'. También aconseja a los usuarios cambiar información confidencial como la contraseña del administrador de ownCloud, las credenciales del servidor de correo y de la base de datos, y las claves de acceso al almacenamiento de objetos/S3.

El segundo problema posibilita el acceso, modificación o eliminación de cualquier archivo sin autenticación, siempre y cuando se conozca el nombre de usuario de la víctima y esta no tenga configurada una clave de firma, que es la configuración predeterminada.

Por último, la tercera vulnerabilidad está relacionada con un caso de control de acceso indebido que permite a un atacante *«introducir una URL de redirección especialmente elaborada que elude el código de validación y, por ende, permite al atacante redirigir devoluciones de llamada a un dominio controlado por este».*

Además de agregar medidas de fortalecimiento al código de validación en la aplicación oauth2, ownCloud ha sugerido a los usuarios desactivar la opción *«Permitir Subdominios»* como solución temporal.

Esta divulgación se produce a medida que se ha difundido un exploit de prueba de concepto (PoC) para una vulnerabilidad crítica de ejecución remota de código en la solución CrushFTP (CVE-2023-43177), que podría ser aprovechada por un atacante no autenticado para acceder a archivos, ejecutar programas arbitrarios en el host y obtener contraseñas en texto plano.

El problema ha sido abordado en la versión 10.5.2 de CrushFTP, lanzada el 10 de agosto de 2023.

> *«Esta vulnerabilidad es crítica porque NO requiere autenticación. Puede realizarse de forma anónima y robar la sesión de otros usuarios, escalando incluso a un usuario administrador»*, señaló CrushFTP en un aviso emitido en ese momento.