BOLETÍN DE ALERTA

Boletín Nro.: 2023-53
Fecha de publicación: 28/11/2023
Tema: Vulnerabilidad en Nextcloud Server permite a usuarios malintencionados inutilizar almacenamiento externo.

Productos afectados:

- versiones anteriores a la 25.0.13, 26.0.8 y 27.1.3 de Nextcloud Server.
- versiones anteriores a la 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8 y 27.1.3 de Nextcloud Enterprise Server.

Descripción:

Se ha detectado una vulnerabilidad en Nextcloud Server que permite a usuarios malintencionados actualizar cualquier almacenamiento externo personal o global, convirtiéndolo en inaccesible para otros usuarios. La vulnerabilidad fue identificada como CVE-2023-48239 con una puntuación asignada de 8.5 CVSS.

Impacto:

Un actor malicioso podría actualizar cualquier almacenamiento externo personal o global haciéndolos inaccesibles para todos los demás usuarios.

Solución:

Se recomienda actualizar Nextcloud Server y Nextcloud Enterprise Server a la versión más reciente.

Recomendación:

Se puede desactivar la aplicación "files_external", lo que hará que el almacenamiento externo sea inaccesible, pero mantendrá las configuraciones hasta que se implemente una versión parcheada.

Información adicional:

- https://www.cvedetails.com/cve/CVE-2023-48239/
- https://github.com/nextcloud/security-advisories/security/advisories/GHSA-f962-hw26-g267