Fortinet ha emitido soluciones para abordar una vulnerabilidad crítica de seguridad que afecta a FortiClientLinux y que podría ser aprovechada para lograr la ejecución de código arbitrario.

Identificado como CVE-2023-45590, el fallo de seguridad tiene una puntuación CVSS de 9.4 sobre un máximo de 10.

> *«Una vulnerabilidad de Control Incorrecto en la Generación de Código ('Inyección de Código') [CWE-94] en FortiClientLinux podría permitir a un atacante no autenticado ejecutar código arbitrario al engañar a un usuario de FortiClientLinux para que visite un sitio web malicioso»,* afirmó Fortinet en un aviso.

La debilidad, catalogada como un caso de ejecución remota de código debido a una *«configuración arriesgada de nodejs»,* afecta a las siguientes versiones:

- Versiones de FortiClientLinux 7.0.3 a 7.0.4 y de 7.0.6 a 7.0.10 (Actualizar a 7.0.11 o superior)
- Versión de FortiClientLinux 7.2.0 (Actualizar a 7.2.1 o superior)

El investigador de seguridad CataLpa de Dbappsecurity ha sido reconocido por descubrir y reportar esta vulnerabilidad.

Los parches de seguridad de Fortinet para abril de 2024 también abordan un problema con el instalador de FortiClientMac que podría resultar en la ejecución de código (CVE-2023-45588 y CVE-2024-31492, puntuaciones CVSS: 7.8).

Asimismo, se ha solucionado un error en FortiOS y FortiProxy que podría provocar la filtración de cookies de administrador en determinados escenarios (CVE-2023-41677, puntuación CVSS: 7.5).

Aunque no se ha detectado evidencia de que estas fallas hayan sido explotadas en la

práctica, se recomienda a los usuarios mantener sus sistemas actualizados para reducir posibles riesgos.