Los actores maliciosos están intentando explotar una vulnerabilidad recientemente descubierta en los firewalls GFI KerioControl que, si se aprovecha con éxito, podría permitir la ejecución remota de código (RCE).

Esta falla, registrada como CVE-2024-52875, está relacionada con un ataque de inyección CRLF (retorno de carro y salto de línea), lo que facilita la división de respuestas HTTP y puede derivar en una vulnerabilidad de tipo XSS (cross-site scripting).

La explotación exitosa de esta debilidad de RCE con un solo clic permite que un atacante inyecte datos maliciosos en los encabezados de respuesta HTTP mediante el uso de caracteres \r y \n.

El investigador de seguridad Egidio Romano, quien identificó y reportó la vulnerabilidad a principios de noviembre de 2024, explicó que afecta a las versiones de KerioControl entre la 9.2.5 y la 9.4.5.

Se detectaron fallas de división de respuestas HTTP en los siguientes caminos URI:

- `/nonauth/addCertException.cs`
- `/nonauth/guestConfirm.cs`
- `/nonauth/expiration.cs`

> *«Los datos introducidos por el usuario a través del parámetro GET 'dest' no se procesan adecuadamente antes de generar un encabezado HTTP 'Location' en una respuesta 302»*, señaló Romano.
>
> *«En particular, la aplicación no filtra ni elimina correctamente los caracteres de salto de línea (LF), lo que permite llevar a cabo ataques de división de respuestas HTTP que podrían derivar en XSS reflejado y otras posibles amenazas».*

GFI publicó un parche para resolver este problema el 19 de diciembre de 2024, lanzando la versión 9.4.5 Patch 1. Desde entonces, se ha hecho público un exploit de prueba de concepto (PoC).

Un atacante podría generar una URL maliciosa que, al ser abierta por un administrador, active el PoC alojado en un servidor bajo control del atacante. Esto podría permitir la carga de un archivo malicioso .img a través de la funcionalidad de actualización de firmware, lo que concedería acceso root al firewall.

Según la firma de inteligencia de amenazas GreyNoise, los primeros intentos de explotar la vulnerabilidad CVE-2024-52875 ocurrieron el 28 de diciembre de 2024, con ataques originados desde siete direcciones IP distintas ubicadas en Singapur y Hong Kong.

El análisis de Censys indica que hay más de 23,800 instancias de GFI KerioControl expuestas a internet. La mayoría de estos servidores se encuentran en Irán, Uzbekistán, Italia, Alemania, Estados Unidos, República Checa, Bielorrusia, Ucrania, Rusia y Brasil.

Aunque aún no se ha determinado con exactitud cómo se están llevando a cabo los ataques, se aconseja a los usuarios de KerioControl que refuercen la seguridad de sus sistemas lo antes posible para reducir los riesgos.