La compañía de seguridad cibernética Sophos advirtió este lunes que una vulnerabilidad crítica de seguridad, parcheada recientemente en su producto de firewall, está siendo explotada activamente en ataques reales.

La vulnerabilidades, registrada como CVE-2022-1040, tiene una calificación de 9.8 en el sistema de puntuación CVSS, e impacta en las versiones de Sophos Firewall 18.5 MR3 (18.5.3) y anteriores.

Se relaciona con una vulnerabilidad de omisión de autenticación en el Portal de usuario y la interfaz Webadmin que, de utilizarse exitosamente, permite que un atacante remoto ejecute código arbitrario.

> *«Sophos ha observado que esta vulnerabilidad se usa para apuntar a un pequeño conjunto de organizaciones específicas principalmente en la región del sur de Asia. Hemos informado a cada una de estas organizaciones directamente»,* dijo la compañía.

La vulnerabilidad se solucionó en una revisión que se instala de forma automática para los clientes que tienen habilitada la configuración «*Permitir la instalación automática de revisiones*«. Como solución alternativa, Sophos recomienda que los usuarios deshabiliten el acceso WAN a las interfaces Portal de usuario y Webadmin.

Además, la compañía envió versiones no compatibles al final de su vida útil, 17.5 MR12 a MR15, 18.0 MR3 y MR4 y 18.5 GA, lo que resalta la gravedad del problema.

> *«Los usuarios de versiones anteriores de Sophos Firewall deben actualizarse para recibir las últimas protecciones y esta solución»,* dijo Sophos.