BOLETÍN DE ALERTA

Boletín Nro.: 2024-09
Fecha de publicación: 09/02/2024
Tema: Vulnerabilidad crítica de seguridad en FortiOS de Fortinet

Productos afectados:
Fortigate/FortiOS versiones:
-7.4.0 hasta 7.4.2
-7.2.0 hasta 7.2.6
-7.0.0 hasta 7.0.13
-6.4.0 hasta 6.4.14
-6.2.0 hasta 6.2.15
-6.0

Descripción:

Fortinet ha lanzado recientemente actualizaciones de seguridad para su sistema operativo FortiOS, utilizado en los firewalls Fortigate, debido a una vulnerabilidad identificada como CVE-2024-21762 con puntuación CVSS 9.8 de severidad crítica, que permiten ejecutar código remoto (RCE).

Impacto:

Esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código o comandos arbitrarios a través de solicitudes HTTP especialmente diseñadas.

Recomendación:

- Actualizar de inmediato los productos afectados, a las versiones que corrigen la vulnerabilidad, siguiendo las indicaciones del fabricante, disponibles en los enlaces de referencia.
- Para dispositivos que exponen servicios SSL-VPN, se aconseja proteger las interfaces de administración segregándolas en segmentos de red accesibles sólo por personal autorizado.
- En caso de no poder actualizar rápidamente los dispositivos expuestos en Internet, se sugiere desactivar temporalmente el servicio SSL-VPN.

Información adicional:

- https://www.fortiguard.com/psirt/FG-IR-24-015
- https://docs.fortinet.com/product/fortigate/7.4
- https://docs.fortinet.com/product/fortigate/7.2
- https://docs.fortinet.com/product/fortigate/7.0
- https://docs.fortinet.com/product/fortigate/6.4