



BOLETÍN DE ALERTA

Boletín Nro.: 2022-51

Fecha de publicación: 14/12/2022

Tema: Explotación activa de vulnerabilidad *RCE* en SSL-VPN Fortinet

Los productos afectados son:

- FortiOS:
 - Versión 7.2.0 a 7.2.2.
 - Versión 7.0.0 a 7.0.8.
 - Versión 6.4.0 a 6.4.10.
 - Versión 6.2.0 a 6.2.11.
 - Versión 6.0.0 a 6.0.15
 - Versión 5.6.0 a 5.6.14
 - Versión 5.4.0 a 5.4.13
 - Versión 5.2.0 a 5.2.15
 - Versión 5.0.0 a 5.0.14
- FortiOS-6K7K:
 - Versión 7.0.0 a 7.0.7.
 - Versión 6.4.0 a 6.4.9.
 - Versión 6.2.0 a 6.2.11.
 - Versión 6.0.0 a 6.0.14.

Descripción:

Recientemente se han reportado incidentes de seguridad sobre una vulnerabilidad crítica de día cero (*0-day*) que afecta a productos de Fortinet, que permitiría a un atacante provocar desbordamiento de búfer y así realizar ejecución remota de código (*RCE*).

La vulnerabilidad identificada como [CVE-2022-42475](#), de severidad "Crítica" y con puntuación asignada de 9.3. Esta vulnerabilidad de día cero (*0-day*) explotada activamente se debe a una falla encontrada en FortiOS SSL-VPN. Un atacante remoto no autenticado podría aprovechar esta vulnerabilidad para provocar desbordamiento de búfer (*heap-based*) a través de una solicitud especialmente diseñada y así realizar ejecución de códigos y comandos arbitrarios en el sistema afectado.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría realizar desbordamiento de búfer y provocar ejecución de códigos y comandos arbitrarios de forma remota.

Ciberseguridad y Protección de la Información

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Gral. Santos y Concordia - Complejo Santos - Offic. E14

cert@cert.gov.py | +595 21 217 9000

Asunción - Paraguay | www.cert.gov.py





Solución:

Recomendamos acceder a la actualización de seguridad correspondiente a través de la siguiente guía provista por Fortinet:

- <https://www.fortiguard.com/psirt/FG-IR-22-398>

Adicionalmente recomendamos en caso de no poder aplicar la actualización, proceder a la deshabilitación del componente SSL-VPN en caso de no ser necesario, posterior análisis.

Información adicional:

- <https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/fortinet-says-ssl-vpn-pre-auth-rce-bug-is-exploited-in-attacks/amp/>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42475>
- <https://www.fortiguard.com/psirt/FG-IR-22-398>