# BOLETÍN DE ALERTA

**Boletín Nro.**: 2023-05
**Fecha de publicación**: 22/02/2023
**Tema**: Múltiples vulnerabilidades en productos Fortinet y *PoC* publicado.

**Algunos productos afectados son:**

- FortiNAC, versión 9.4.0.
- FortiNAC, versión 9.2.0 hasta 9.2.5.
- FortiWeb, versión 6.0.7 y anteriores.
- FortiWeb, versión 6.1.2 y anteriores.

**Descripción:**

Se han reportado nuevos avisos de seguridad sobre una nueva prueba de concepto (*PoC) e* indicadores de compromiso *(IoC)* que han sido publicados correspondientes a una vulnerabilidad crítica que afecta al producto FortiNAC de Fortinet, que permitiría a un atacante realizar ejecución arbitraria de código en un sistema vulnerable. La misma fue publicada anteriormente en una noticia en la cual se reportan múltiples vulnerabilidades.

Se han recibido reportes de *exploit* liberados al público que explotan principalmente la vulnerabilidad CVE-2022-39952. Recomendamos tomar medidas correctivas contra estas vulnerabilidades los más pronto posible.

Las mismas se componen de 2 (dos) vulnerabilidades de severidad “Crítica”, 15 (quince) de severidad “Alta”, 19 (diecinueve) de severidad “Media” y 3 (tres) de severidad “Baja” según el fabricante. Las principales se detallan a continuación:

- CVE-2022-39952, de severidad “Crítica”, con puntuación de 9.8. Esta vulnerabilidad con *IoC* y *PoC público* se debe a una falla de seguridad en el control de los nombres de archivos o rutas del servidor web en FortiNAC. Esto permitiría a un atacante no autenticado realizar acciones de escritura sobre archivos de forma arbitrariay desencadenar en una posible ejecución de código arbitrario en el sistema afectado.

- CVE-2021-42756, de severidad “Crítica”, con puntuación de 9.3. Esta vulnerabilidad del tipo *stack-based buffer overflow* se debe a una falla de seguridad en el *proxy daemon* de FortiWeb. Esto permitiría a un atacante remoto y no autenticado a través del envío de peticiones *HTTP* específicamente diseñadas, realizar la ejecución código arbitrario en el sistema vulnerable.

- CVE-2023-25602, de severidad “Alta”, con puntuación de 7.4 Esta vulnerabilidad del tipo *stack-based buffer overflow* se debe a la incorrecta gestión de memoria por parte de la línea de comandos de FortiWeb. Esto permitiría a un atacante autenticado a través del envío de comandos específicamente diseñados, ejecutar código o comandos arbitrarios en el sistema vulnerable.

Puede acceder a la lista completa de los productos afectados en el siguiente enlace.

**Impacto:**

La explotación exitosa de estas vulnerabilidades permitiría a un atacante realizar escritura arbitraria de archivos, ejecutar código o comandos arbitrarios, entre otros.

**Solución:**

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante, acorde a la tecnología afectada indicada en el siguiente enlace:

- https://www.fortiguard.com/psirt?date=02-2023
- https://www.fortinet.com/support/product-downloads

**Información adicional:**

- https://www.cert.gov.py/noticias/vulnerabilidades-de-ejecucion-arbitraria-de-codigo-e-inyeccion-de-comandos-en-productos-fortinet/
- https://www.bleepingcomputer.com/news/security/exploit-released-for-critical-fortinet-rce-flaws-patch-now/
- https://securityonline.info/poc-for-cve-2022-39952-affecting-fortinet-fortinac-published/
- https://blog.segu-info.com.ar/2023/02/fortinet-soluciona-40-fallas-2-criticas.html
- https://github.com/horizon3ai/CVE-2022-39952
- https://www.horizon3.ai/fortinet-fortinac-cve-2022-39952-deep-dive-and-iocs/
- https://nvd.nist.gov/vuln/detail/CVE-2022-39952
- https://www.fortiguard.com/psirt/FG-IR-22-300
- https://securityaffairs.com/142553/hacking/poc-exploit-code-fortinet-fortinac.html
- https://www.fortiguard.com/psirt?page=1&date=02-2023