# BOLETÍN DE ALERTA

**Boletín Nro.**: 2023-30
**Fecha de publicación**: 14/06/2023
**Tema**: Vulnerabilidad RCE en productos Fortinet.

**Algunos de los productos afectados son:**

- FortiOS-6K7K, versiones 7.0.10, 7.0.5, 6.4.12, entre otras.
- FortiProxy SSL-VPN 1.1 y 1.2, todas las versiones.
- FortiOS versiones 7.2.0 a 7.2.4, 7.0.0 a 7.0.11, 6.4.0 a 6.4.12, entre otras.
- FortiADC, versión 7.1.0 a 7.1.2.
- FortiNAC, versión 9.4.0 a 9.4.1.

Se puede acceder al listado completo de productos afectados aquí

**Descripción:**

Se han reportado nuevos avisos de seguridad sobre vulnerabilidades que afectan a productos Fortinet: FortiOS y FortiProxy.

Las vulnerabilidades reportadas se componen de 1 (una) de severidad “Crítica”, 7 (siete) de severidad “Alta”, 11 (once) de severidad “Media” y 2 (dos) de severidad “Baja”. Las principales se detallan a continuación:

- CVE-2023-27997, de severidad “Crítica” y con puntuación asignada de 9.8. Esta vulnerabilidad del tipo *heap-based buffer overflow* se debe a una falla de seguridad en SSL-VPN de FortiOS y FortiProxy. Esto permitiría a un atacante remoto no autenticado a través de una solicitud especialmente diseñada, realizar ejecución de código o comandos arbitrarios en los productos afectados.

- CVE-2023-26210, de severidad “Alta” y con puntuación asignada de 7.8. Esta vulnerabilidad del tipo *OS Command Injection* se debe a la incorrecta validación de caracteres especiales en FortiADC y FortiADC Manager. Esto permitiría a un atacante local autenticado a través de solicitudes *CLI* especialmente diseñadas, realizar ejecución de código de *shell* arbitrario como usuario *root* en los productos afectados.

- CVE-2023-22633, de severidad “Alta” y con puntuación asignada de 7.5. Esta vulnerabilidad se debe a una falla de gestión apropiada de permisos, privilegios y controles de acceso en FortiNAC. Esto permitiría a un atacante remoto no autenticado realizar ataques de denegación de servicios (*DoS*) en el dispositivo a través de la renegociación segura del cliente.

Se puede acceder al boletín de seguridad publicado por la empresa Fortinet en el siguiente enlace:

- https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign

**Se recomienda tomar acción rápidamente dado que existen reportes de que la vulnerabilidad CVE-2023-27997 está siendo explotada activamente.**

**Impacto:**

La explotación exitosa de la vulnerabilidad más crítica podría permitir a un atacante remoto no autenticado obtener el control total del sistema afectado.

**Solución:**

Puede corroborar en el siguiente enlace cual sería la actualización que corresponde a su equipo:

- https://www.fortiguard.com/psirt/FG-IR-23-097

En el siguiente enlace puede acceder a las actualizaciones correspondientes provistas por el fabricante:

- https://docs.fortinet.com/upgrade-tool

**Mitigación:**

Se recomienda deshabilitar el *SSL-VPN* para los productos Fortinet. Esta opción no se encuentra activada por defecto en los dispositivos.

**Información adicional:**

- https://www.fortiguard.com/psirt/FG-IR-23-097
- https://thehackernews.com/2023/06/critical-fortios-and-fortiproxy.html
- https://labs.watchtowr.com/xortigate-or-cve-2023-27997/
- https://nvd.nist.gov/vuln/detail/CVE-2023-27997
- https://nvd.nist.gov/vuln/detail/CVE-2023-22633
- https://nvd.nist.gov/vuln/detail/CVE-2023-26210

- https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign
- https://securityonline.info/cve-2023-27997-fortinet-fortigate-pre-auth-rce-vulnerability/
- https://www.fortiguard.com/psirt
- https://www.fortiguard.com/psirt/FG-IR-23-076
- https://www.fortiguard.com/psirt/FG-IR-22-521