Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

FORTINET CORRIGE FALLO CRÍTICO DE RCE EN LOS DISPOSITIVOS SSL-VPN DE FORTIGATE

13 / Junio /2023

CONTENIDO

INTRODUCCIÓN

Fortinet ha lanzado una nueva ronda de actualizaciones de emergencia para el firmware de Fortigate, los parches mitigan la vulnerabilidad crítica CVE-2023-27997 (CVSSv3 9.2), la cual conduce a la ejecución remota de código (previo a la autenticación) en dispositivos FortiOS SSL VPN, incluso si MFA está habilitado.

Los dispositivos de Fortinet son algunos de los Firewalls y VPN más populares del mercado, lo que los convierte en un objetivo habitual de los ataques, por tanto, los administradores deben aplicar las actualizaciones de seguridad de Fortinet tan pronto sea posible.

FORTINET

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_06_13_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	13/06/2023
Es día cero (0 day):	No

GENERALIDADES

Fortinet ha liberado actualizaciones del firmware de Fortigate, estas actualizaciones tienen como objetivo, corregir la vulnerabilidad crítica no divulgada, de ejecución remota de código, previo a la autenticación en dispositivos VPN SSL.

La vulnerabilidad en cuestión ha sido rastreada como CVE-2023-27997. Y las correcciones para cubrirla han sido publicadas el pasado viernes 9 de junio. Las versiones de firmware son FortiOS 6.0.17, 6.2.15, 6.4.13, 7.0.12 y 7.2.5.

Si bien, no se menciona en las notas de la versión, profesionales de ciber seguridad y los administradores han insinuado que las actualizaciones corregían sin llamar la atención, una vulnerabilidad crítica SSL-VPN RCE que se revelaría el martes 13 de junio de 2023.

El hecho de liberar el parche antes de si quiera hacer mención o publicar la información relacionada a la vulnerabilidad, no es una práctica poco común, por parte de Fortinet, pues estos liberan el parche previo a la CVE, de manera que los usuarios puedan actualizar los dispositivos antes de que cualquier atacante pueda hacer ingeniería inversa de los parches.

Según informa Charles Fol, de Lexfo Security. Las nuevas actualizaciones de FortiOS incluyen una corrección para una vulnerabilidad RCE crítica descubierta por él y Rioru.

Imagen 1. Cuenta oficial de Fol, sobre vulnerabilidad descubierta por el y Dany Bach.

Según lo haría saber el investigador, por medio de su cuenta oficial de Twitter. “Fortinet publicó un parche para CVE-2023-27997, vulnerabilidad de ejecución remota de código, de la cual @DDXhunter y yo informamos”. También hacia saber “Esto es accesible pre-autenticación, en cada dispositivo SSL VPN”, y terminaba su publicación instando a los usuarios a parchear su Fortigate.

Según habría declarado Fol, esta vulnerabilidad debe ser parchada de manera urgente, para administradores de Fortinet, pues según este, es muy probable que la vulnerabilidad sea rápidamente analizada y descubierta por actores de amenazas.

VULNERABILIDAD

Una vulnerabilidad de desbordamiento de búfer basada en heap [CWE-122] en FortiOS y FortiProxy SSL-VPN puede permitir a un atacante remoto ejecutar código o comandos arbitrarios a través de solicitudes específicamente diseñadas.

Según la empresa francesa de ciberseguridad Olympe Cyberdefense, la vulnerabilidad rastrada como CVE-2023-27997 permitiría a un agente malicioso interferir a través de la VPN, incluso si la MFA está activada. También menciona que, a la fecha, todas las versiones estarían afectadas, y mencionaba estar a la expectativa para la publicación del CVE el martes 13 de junio.

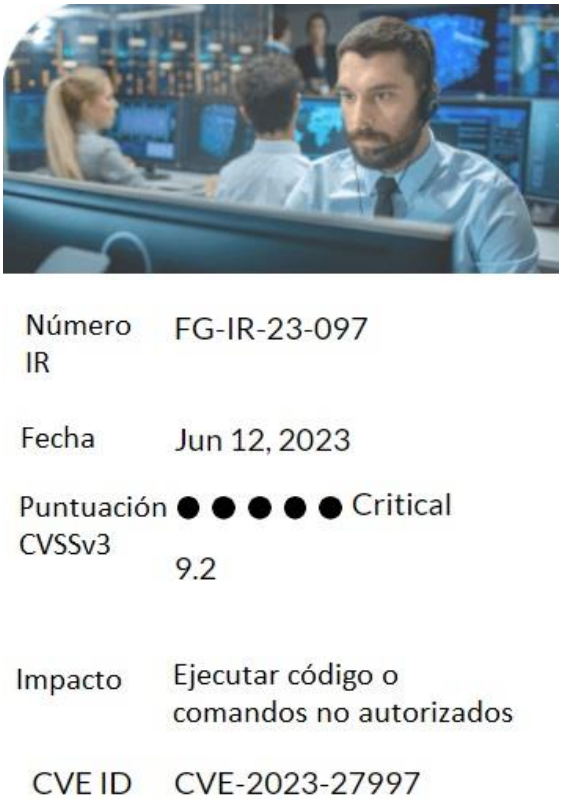

Imagen 2. Puntuación CVSS según comunicado de FortiGuard Labs.

PANORAMA MUNDIAL

Según informes de Shodan, los dispositivos FortiGate de Fortinet, suponen alrededor de 564,750 instancias, alrededor del mundo, de las cuales, una gran mayoría (como se presenta más detalladamente más abajo en este informe) se encuentran vulnerables.

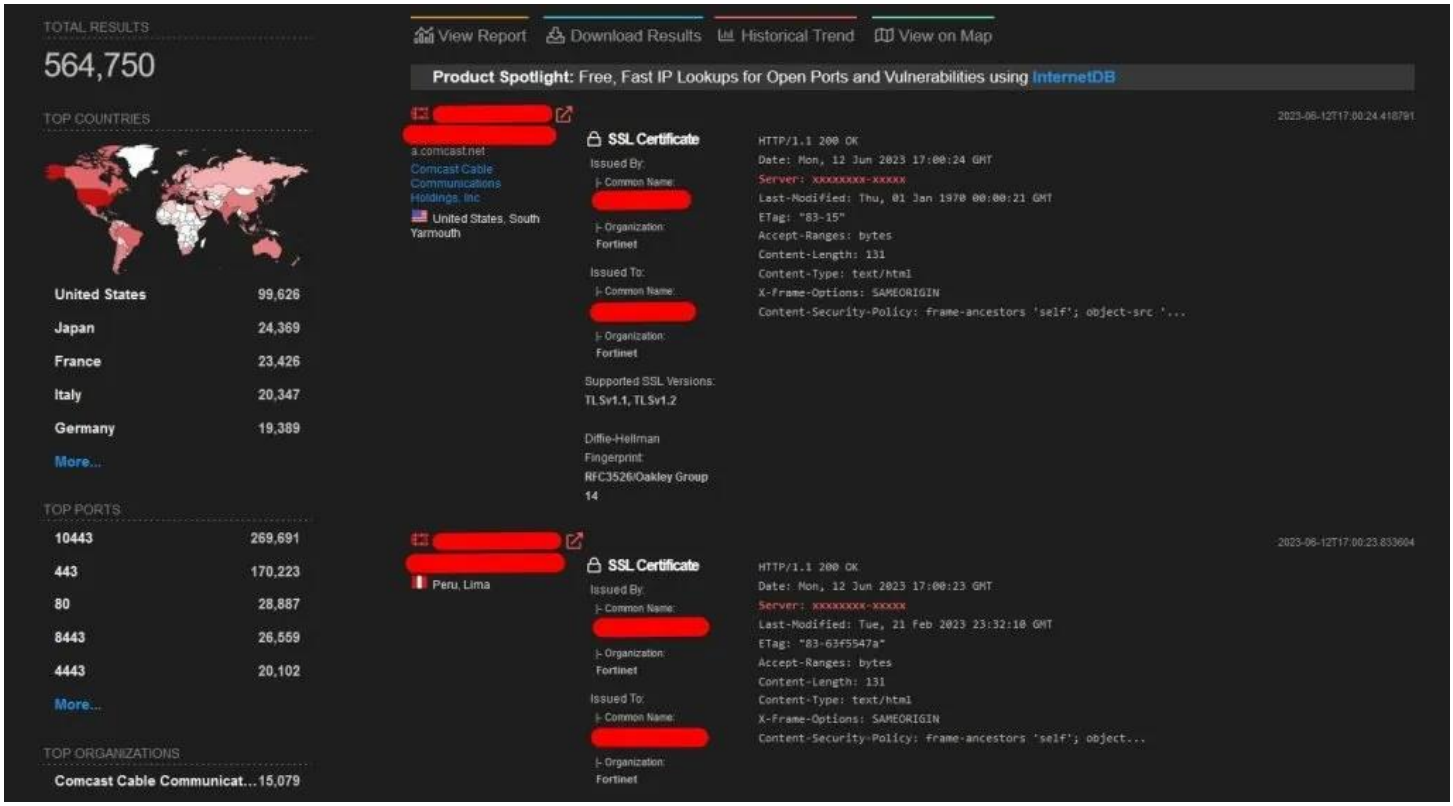

Imagen 3. Instancias Fortinet según Shodan.

La importancia de esta vulnerabilidad radica en que los dispositivos Fortinet son algunos de los Firewalls y VPN más utilizados en el sector, lo que lo vuelve un objetivo frecuente de ataques por parte de actores maliciosos.

El fallo afecta a todas las versiones anteriores a parcheo, lo cual resulta alarmante, pues según una búsqueda en Shodan, se puede acceder a más de 250 mil firewalls Fortigate desde internet, sumado a lo anterior, se puede llegar a la conclusión que la gran mayoría de firewalls Fortigate se encuentren expuestos.

Se tiene precedentes de explotación de vulnerabilidades de SSL-VPN posterior a la liberación de los parches, que suelen utilizarse para obtener acceso inicial a las redes, con la finalidad de realizar robo de datos y en una situación más crítica, ataques de ransomware. De manera que la aplicación de los parches de Fortinet, se deben llevar a cabo por los administradores, de manera inmediata, según disponibilidad de los parches en cuestión

IBEROAMERICA

EL Panorama para el caso de Iberoamérica, resulta de igual manera, alarmante, pues se tiene un conteo de cerca de 78,520 instancias de FortiGate potencialmente vulnerables, de distribución de estas se presenta a continuación:

PAÍS	INSTANCIAS
BR	17.968
ES	14.054
MX	10.936
PE	8.623
AR	7.472
CO	5.845
CL	4.421
EC	2.066
PR	1.672
PA	1.207
UY	1.103
VE	1.081
PY	979
HN	598
BO	494

Imagen 4. Instancias de Fortinet en Iberoamérica.

Según declaraciones que hiciera Fortinet, en relación con la explotación de esta vulnerabilidad. La compañía expreso:

“La comunicación oportuna y continua con nuestros clientes es un componente clave de nuestros esfuerzos para proteger y asegurar mejor su organización. Hay casos en los que las comunicaciones confidenciales anticipadas con los clientes pueden incluir advertencias tempranas sobre avisos para permitir a los clientes reforzar aún más su postura de seguridad, antes de que el aviso se divulgue públicamente a un público más amplio. Este proceso sigue las mejores prácticas de divulgación responsable para garantizar que nuestros clientes tengan la información oportuna que necesitan para ayudarles a tomar decisiones informadas basadas en el riesgo. Para más información sobre el proceso de divulgación responsable de Fortinet, visite la página del Equipo de Respuesta a Incidentes de Seguridad de Productos de Fortinet (PSIRT): https://www.fortiguard.com/psirt_policy."

PRODUCTOS AFECTADOS

Según ha revelado Fortinet, algunos de los productos afectados serían los que se listan a continuación:

- FortiOS-6K7K versión 7.0.10
- FortiOS-6K7K versión 7.0.5
- FortiOS-6K7K versión 6.4.12
- FortiOS-6K7K versión 6.4.10
- FortiOS-6K7K versión 6.4.8
- FortiOS-6K7K versión 6.4.6
- FortiOS-6K7K versión 6.4.2
- FortiOS-6K7K versión 6.2.9 hasta 6.2.13
- FortiOS-6K7K versión 6.2.6 hasta 6.2.7
- FortiOS-6K7K versión 6.2.4
- FortiOS-6K7K versión 6.0.12 hasta 6.0.16
- FortiOS-6K7K versión 6.0.10
- FortiProxy versión 7.2.0 hasta 7.2.3
- FortiProxy versión 7.0.0 hasta7.0.9
- FortiProxy versión 2.0.0 hasta 2.0.12
- FortiProxy 1.2 todas las versiones
- FortiProxy 1.1 todas las versiones
- FortiOS versión 7.2.0 hasta7.2.4
- FortiOS versión 7.0.0 hasta 7.0.11
- FortiOS versión 6.4.0 hasta 6.4.12
- FortiOS versión 6.2.0 hasta 6.2.13
- FortiOS versión 6.0.0 hasta 6.0.16

RECOMENDACIONES

El proveedor recomienda la actualización de los equipos de manera inmediata. Como una alternativa temporal también recomienda deshabilitar SSL-VPN. A continuación, se presenta las versiones según lo indica el proveedor:

- FortiOS versión 7.2.0 hasta 7.2.4
- FortiOS-6K7K versión 7.0.12 o superior
- FortiOS-6K7K versión 6.4.13 o superior
- FortiOS-6K7K versión 6.2.15 o superior
- FortiOS-6K7K versión 6.0.17 o superior
- FortiProxy versión 7.2.4 o superior
- FortiProxy versión 7.0.10 o superior
- FortiOS versión 7.4.0 o superior
- FortiOS versión 7.2.5 o superior
- FortiOS versión 7.0.12 o superior
- FortiOS versión 6.4.13 o superior
- FortiOS versión 6.2.14 o superior
  FortiOS versión 6.0.17 o superior

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente