Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

FORTINET: FALLAS CRITICAS PODRIAN CONDUCIR A ATAQUES RCE

13 / julio /2023

CONTENIDO

INTRODUCCIÓN

Fortinet ha anunciado recientemente el descubrimiento de una falla critica en FortiOS y FortiProxy, la cual permite a un actor de amenazas realizar ataques de ejecución remota de código. La vulnerabilidad ha sido rastreada como CVE-2023-33308, y ha sido catalogada como critica, asignándosele una puntuación CVSSv3 de 9.8/10 lo cual refleja la criticidad de este.

La vulnerabilidad de RCE en cuestión se da en el margen de explotación activa de una vulnerabilidad que fuera parcheada el 11 de junio del 2023, según se ha podido observar, alrededor de 300,000 dispositivos se encontrarían aun vulnerables, resultado de una mala gestión de actualización por parte de administradores.

FORTINET

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

ID de alerta:	DSOC-CERT_2023_07_13_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	13/07/2023
Es día cero (0 day):	No

VULNERABILIDAD

Falla critica en dispositivos FortiOS y FortiProxy de Fortinet permitirías a actores maliciosos conducir ataques de ejecución de código remota en dispositivos vulnerables.

La vulnerabilidad en cuestión ha sido rastreada como CVE-2023-33308 y ha sido reportada por el equipo de Watchtowr. CVE-2023-33308, es una vulnerabilidad de desbordamiento basada en pila en instancias de FortiOS y FortiProxy, se produce cuando el software que escribe datos en un búfer desborda la capacidad del búfer, lo que provoca que se sobrescriban las ubicaciones de memoria adyacente. La vulnerabilidad ha sido catalogada como critica, asignándosele una puntuación de CVSSv3 9.8/10, lo que refleja dicha criticidad.

Número IR	FG-IR-23-183
Fecha	Jul 11, 2023
Severidad	●●●●● Critico
Puntuación CVSSv3	9.8
Impacto	Ejecución de código o comandos no autorizado
CVE ID	CVE-2023-33308
Productos afectados	FortiOS : 7.2.3, 7.2.2, 7.2.1, 7.2.0, 7.0.10, 7.0.9, 7.0.8, 7.0.7, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0 FortiProxy : 7.2.2, 7.2.1, 7.2.0, 7.0.9, 7.0.8, 7.0.7, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0
CVRF	Download

Imagen 1. Resumen vulnerabilidad CVE-2023-33308.

Un desbordamiento de búfer permite a un atacante remoto ejecutar código arbitrario a través de paquetes especialmente diseñados los cuales alcanzan políticas del proxy o bien del firewall, modo proxy junto con la inspección profunda de paquetes SSL.

PRODUCTOS AFECTADOS

Las versiones de FortiOS afectadas, se describen a continuación:

- FortiOS verión 7.2.0 hasta 7.2.3
- FortiOS versión 7.0.0 hasta 7.0.10

Las versiones de Forti Proxy afectadas se describen a continuación:

- FortiProxy versión 7.2.0 hasta 7.2.2
- FortiProxy versión 7.0.0 hasta 7.0.9

Según lo comenta la empresa, el problema se habría abordado en una versión anterior, por lo que la vulnerabilidad CVE-2023-33308 no afectaría las últimas versiones FortiOS 7.4. Las versiones destinadas a solucionar los problemas derivados de la vulnerabilidad en cuestión son las siguientes:

- FortiOS versión 7.4.0 o superior.
- FortiOS versión 7.2.4 o superior.
- FortiOS versión 7.0.11 o superior.
- FortiProxy versión 7.2.3 o superior.
- FortiProxy versión 7.0.10 o superior.

A su vez, Fortinet mencionaba en que todas las versiones de FortiOS 6.4, 6.2, 6.0; así como todas las versiones de FortiProxy 2.x y 1.x, no se verían afectadas por CVE-2023-33308.

WORKAROUND

Referente a CVE-2023-33308, Fortinet proporcionaba una solución alternativa, la cual consiste en deshabilitar la compatibilidad con HTTP/2 en perfiles de inspección SSL utilizados por políticas proxy o políticas de cortafuegos con modo proxy. Fortinet proporciona el siguiente ejemplo con perfil de inspección profunda personalizado:

```
config firewall ssl-ssh-profile
   edit "custom-deep-inspection"
      set supported-alpn http1-1
   next
end
```

Imagen 2. perfil de inspección profunda personalizada.

OTRAS VULNERABILIDADES

El anuncio de CVE-2023-33308 en el margen de otros problemas relacionados a una vulnerabilidad ya parcheada en firewalls de FortiGate, rastreada como CVE-2023-27997. La empresa Bishop Fox recalcaba el hecho que, aunque la vulnerabilidad ya había sido parcheada por Fortinet, aun existían más de 300,000 firewalls de FortiGate, vulnerables a ataques conducidos por actores maliciosos, aprovechando CVE-2023-27997.

CVE-2023-27997 es explotable y permite a un atacante no autenticado ejecutar código de forma remota en dispositivos vulnerables con la interfaz SSL VPN expuesta en la web. En un aviso de mediados de junio, el fabricante advirtió de que el problema podía haber sido explotado en ataques.

```
$ shodan count '"Server: xxxxxxxx-xxxxx" http.html:"top.location=/remote/login"'
489337
```

Imagen 3. Query de Shodan que para la búsqueda de dispositivos expuestos.

La consulta anterior muestra 489.337 dispositivos, pero no todos eran vulnerables a CVE-2023-27997, también conocido como Xortigate. Investigando más a fondo, los investigadores descubrieron que 153.414 de los dispositivos descubiertos habían sido actualizados a una versión segura de FortiOS.

RECOMENDACIONES

La empresa de software, dispositivos y servicios de ciberseguridad hace un llamado a todos los usuarios a realizar las actualizaciones pertinentes en los sistemas que incluyan las versiones expuestas antes mencionadas, hacia las versiones indicadas por Fortinet.

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