Nro. Alerta:	AL-2023-006	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	24-ene-2023	**Vulnerabilidad en dispositivos Fortinet utilizada para propagar ransomware**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Explotación de vulneraciones conocidas

Nivel de riesgo: Alto

II. ALERTA

Los actores de amenazas han explotado los dispositivos de red privada virtual (VPN) de Fortinet para intentar infectar con ransomware una universidad con sede en Canadá y una empresa de inversión global.

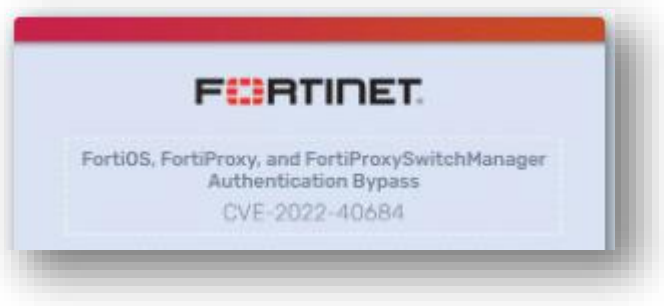

Figura 1.- ***Productos de fortinet vulnerables***
Fuente: https://www.horizon3.ai/fortios-fortiproxy-and-fortiswitchmanager-authentication-bypass-technical-deep-dive-cve-2022-40684/

III. INTRODUCCIÓN

El 10 de octubre de 2022, Fortinet, emitió un comunicado de seguridad revelando que se ha identificado una vulnerabilidad crítica que afectaba a los productos FortiOS, FortiProxy y FortiSwitchManager,

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	AL-2023-006	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	24-ene-2023	**Vulnerabilidad en dispositivos Fortinet utilizada para propagar ransomware**	V 1.1

Fortinet describió a la vulnerabilidad correspondiente al CVE-2022-40684 (puntaje CVSS: 9.6), como una vulnerabilidad de omisión de autenticación; un atacante no autenticado podría obtener acceso a un dispositivo Fortinet vulnerable y realizar alteración de las configuraciones de la red, crear nuevos usuarios, interceptación del tráfico de la red e incluso con movimientos laterales ingresar a la red gracias al uso del protocolo ligero de acceso a directorios (LDAP) y Active Directory (AD).

El 13 de octubre de 2022, en una prueba de concepto (POC) se hizo público el código de explotación con lo cual, los investigadores de ESentire observaron una gran cantidad de actores de amenazas escaneando Internet en busca de dispositivos Fortinet vulnerables. Al realizar búsquedas en la Dark Web, los investigadores observaron a personas malintencionadas que compraban y vendían dispositivos Fortinet comprometidos, lo que indica una explotación generalizada, un resultado típico cuando los detalles técnicos y el conocimiento del código de explotación se hacen públicos y varios actores de amenazas comienzan a participar en la explotación.

La operación de explotación parecía incluir la explotación de vulnerabilidades más antiguas, como CVE-2018-13374, ya que los dispositivos Fortinet desactualizados no eran vulnerables a la vulnerabilidad 2022.

Al realizar búsquedas de amenazas, los investigadores de eSentire revisaron los registros históricos de los dispositivos de Fortinet en busca de indicadores de compromiso e identificaron a varios clientes cuyos dispositivos mostraban signos de actividad de amenazas reciente. En un caso, el intermediario de acceso inicial parecía haber probado su acceso utilizando una carga útil benigna, la aplicación Calculadora de Microsoft.

El Centro de operaciones de seguridad de eSentire respondió a un ataque de ransomware en curso derivadas de dispositivos Fortinet vulnerables dirigido a una Universidad con sede en Canadá y una empresa de inversión global. No se conoce si los actores del ransomware compraron el acceso a través de un agente de acceso inicial o si llevaron a cabo los ataques ellos mismos.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	AL-2023-006	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	24-ene-2023	**Vulnerabilidad en dispositivos Fortinet utilizada para propagar ransomware**	V 1.1

IV. VECTOR DE ATAQUE:

Los actores de amenazas del ransomware, utilizaron el servicio de Protocolo de escritorio remoto (RDP) de Microsoft aprovechando los procesos confiables de Windows (también conocidos como LOLBIN o living-off-the), para lograr movimientos laterales. Los ciberdelincuentes también aprovecharon de las utilidades de cifrado legítimas de BestCrypt y BitLocker.

Los operadores de ransomware presentaron una nota de rescate que siguió el formato de un ransomware observado a principios de 2022 conocido como **Kalaj Tomorr** y tomaron varios pasos para minimizar su identidad:

- Utilizaron herramientas de encriptación legítimas en lugar de ransomware especialmente diseñado. Ellos incluyeron:
    - BestCrypt un cifrador disponible comercialmente, se utiliza para bloquear archivos individuales.
    - BitLocker la utilidad de cifrado nativa de Windows; BitLocker está diseñado para cifrar toda la unidad de disco, incluido el propio sistema operativo y todos los datos del usuario.
- Los intrusos establecieron la contraseña de administrador para la escalada de privilegios.

V. IMPACTO:

FortiLab Guard Labs ha confirmado que la vulnerabilidad afecta a los siguientes productos Fortinet FortiOS, FortiProxy y FortiSwitchManager.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	AL-2023-006	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	24-ene-2023	**Vulnerabilidad en dispositivos Fortinet utilizada para propagar ransomware**	V 1.1

IR Number	FG-IR-22-377
Date	Oct 10, 2022
Severity	●●●●● Critical
CVSSv3 Score	9.6
Impact	Execute unauthorized code or commands
CVE ID	CVE-2022-40684
Affected Products	FortiOS : 7.2.1, 7.2.0, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0 FortiProxy : 7.2.0, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0 FortiSwitchManager : 7.2.0, 7.0.0
CVRF	Download

Figura 2.- ***Versiones de productos Fortinet vulnerables***
Fuente: https://www.fortiguard.com/psirt/FG-IR-22-377

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Realizar las actualizaciones sugeridas por el fabricante.
- No instale aplicaciones de software a menos que sepa exactamente qué es y qué hace.
- Use el principio de privilegio mínimo para que solo los usuarios que necesitan acceso a ciertos datos lo tengan, ese acceso se quita después de un cierto período de tiempo o expira tan pronto como se completa la tarea.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	AL-2023-006	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	24-ene-2023	**Vulnerabilidad en dispositivos Fortinet utilizada para propagar ransomware**	V 1.1

- Implemente la segmentación de la red para que, si un sistema está infectado, pueda aislarse fácilmente del resto de las redes y así garantizar que el ransomware no se propague por la red.
- Realice copias de seguridad de todos sus datos periódicamente y almacene las copias de seguridad por separado, garantizando que NO se pueda acceder a los respaldos desde su red.
- La administración web (HTTPS) publicado al internet debe desactivarse inmediatamente y usarse de manera local hasta que se pueda realizar la actualización.

VII. REFERENCIAS:

Ehacking. (18 de oct de 2022). *Ehcgroup*. Obtenido de https://blog.ehcgroup.io/2022/10/18/10/33/12/14136/exploit-poc-lanzado-para-error-critico-de-omision-de-autenticacion-a-fortinet/noticias-de-seguridad/ehacking/

Esentire. (05 de ene de 2023). *Esentire*. Obtenido de https://www.esentire.com/blog/hackers-exploit-fortinet-devices-to-spread-ransomware-within-corporate-environments-warns-esentire

Fortinet. (s.f.). *Fortiguard Labs Fortinet*. Obtenido de https://www.fortiguard.com/psirt/FG-IR-22-377

horizon3.ai. (13 de Oct de 2022). *horizon3.ai*. Obtenido de https://www.horizon3.ai/fortios-fortiproxy-and-fortiswitchmanager-authentication-bypass-technical-deep-dive-cve-2022-40684/

Infosecurity. (s.f.). *Alessandro Mascellino*. Obtenido de https://www.infosecurity-magazine.com/news/fortinet-devices-distribute/