Alerta de seguridad cibernética	9VSA20-00252-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de junio de 2020
Última revisión	24 de junio de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de FortiNet referente a seis vulnerabilidades que afectan a múltiples de sus productos. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2019-6693
CVE-2020-9289
CVE-2020-9288
CVE-2015-0279
CVE-2020-6644
FG-IR-20-036

CVE-2020-6693

Si la configuración CLI está expuesta (por ejemplo, publicada en un foro para temas de reparación de errores), sería posible para cualquier usuario que tenga acceso, desencriptar los datos de tipo "ENC" a texto plano, utilizando una contraseña criptográfica embebida (hard-coded cryptographic key). También aplica para el archivo de respaldo, si es que no está protegido por una clave.

Productos Afectados

FortiOS versión 6.2.0, desde la 6.0.0 hasta la 6.0.6, y 5.6.10 y anteriores.
(Afecta a todos los datos de credenciales de tipo "ENC" en la configuracioón de FortiOS CLI, excepto a la clave del administrador).

Mitigación

En las versiones 5.6.11, 6.0.7 y 6.2.1 (y superiores) los administradores pueden elegir requerir una contraseña para el acceso a la configuración CLI, la cual es utilizada por FortiOS para encriptar datos sensibles en el archivo de configuración.
Los pasos para activar la contraseña son:
 # config system global
 # set private-data-encryption enable / desactivada por defecto*/*
 # end

Enlaces

https://fortiguard.com/psirt/FG-IR-19-007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6693

CVE-2020-9289

Si la configuración CLI está expuesta (por ejemplo, publicada en un foro para temas de reparación de errores), sería posible para cualquier usuario que tenga acceso, desencriptar los datos de tipo "ENC" a texto plano, utilizando una contraseña criptográfica embebida (hard-coded cryptographic key). También aplica para el archivo de respaldo, si es que no está protegido por una clave.

Productos Afectados

FortiManager versión 6.2.3 y anteriores.
(Afecta a todos los datos de credenciales de tipo "ENC" en la configuracioón de FortiManager CLI).

Mitigación

Actualizar a la versión 6.2.4 o superior de FortiManager, o activar la configuración CLI recientemente introducida, para solicitar una clave criptográfica definida por el usuario. Esa clave se utilizará para cifrar los datos de tipo "ENC" en la configuración:
 # configure system global
 # set private-data-encryption enable / desactivada por defecto*/*
 # end

Enlaces
https://fortiguard.com/psirt/FG-IR-19-007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9289

CVE-2020-9288

Debido a la incorrecta neutralización de datos ingresados en FortiWLC podría permitir a un atacante remoto y autenticado realizar un ataque XSS (Cross-site Scripting) a través de "ESS profile" o "Radius Profile", permitiéndole ejecutar código de forma no autorizada en el servicio afectado.

Productos Afectados
FortiWLC versión 8.5.1 y anteriores.

Mitigación
Actualizar a la versión 8.5.2 o superior de FortiWLC.

Enlaces
https://fortiguard.com/psirt/FG-IR-20-016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9288

CVE-2020-0279

Debido a una vulnerabilidad de tipo inyección de expresión de lenguaje, un atacante remoto podría inyectar código javascript arbitrario en el explorador de una víctima en el contexto de "JBoss RichFaces library".

Productos Afectados
FortiSIEM versión 5.2.8 y anteriores.

Mitigación
Actualizar a la versión 5.3.0 o superior de FortiSIEM.

Enlaces
https://fortiguard.com/psirt/FG-IR-20-041
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0279

CVE-2020-6644

Al no expirar la ID de sesión después de desconectarse en FortiDeceptor, un atacante podría reutilizar la ID no-expirada de un administrador para obtener sus privilegios (si es que logra obtener la ID via otros medios).

Productos Afectados

FortiDeceptor versión 3.0.0 y anteriores.

Mitigación

Actualizar a la versión 3.1.0 o superior de FortiDeceptor.

Enlaces

https://fortiguard.com/psirt/FG-IR-20-006
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6644

FG-IR-20-036

Un insuficiente control del volúmen de mensajes en red podría permitir a un atacante remoto no-autenticado realizar un ataque de amplification NTP (causando una denegación de servicios en destinos arbitrarios), esto a a través de enviar 6 consultas especialmente diseñadas al servidor NTP de FortiAnalyzer.

Productos Afectados

FortiAnalyzer versión 6.4.0, 6.2.3 y anteriores*.
(*) solo modelos que utilicen "FortiRecorder management" son afectados:
FAZ_200F
FAZ_300F
FAZ_400E
FAZ_800F
FAZ_1000E
FAZ_1000F
FAZ_2000E
FAZ_3000F
FAZ_3500G
FAZ_3700F
FAZ_VM64
FAZ_VM64_KVM

Mitigación

Actualizar a la versión 6.2.4 o 6.4.1 de FortiAnalyzer.

Enlaces

https://fortiguard.com/psirt/FG-IR-20-036