Alerta de seguridad cibernética	9VSA20-00272-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de julio de 2020
Última revisión	17 de julio 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 del PSIRT de Fortinet respecto a múltiples vulnerabilidades que afectan a FortiOS, FortiManager, FortiGate, FortiAP y FortiAnalyzer. El presente informe incluye las respectivas medidas de mitigación.

Vulnerabilidades

CVE-2004-1653
CVE-2019-17655
CVE-2019-9193
CVE-2019-6693
CVE-2020-9289
CVE-2020-12812

CVE-2004-1653

Debido a un inapropiado control de acceso en la consola de administrador SSH, un atacante podría acceder a servicios de sistema internos utilizando la redirección de puertos local de SSH. Para un ataque exitoso es necesario que un administrador de consola SSH autenticado configure un rebote en el puerto hacia productos de servicios internos a través de la redirección de puertos. Potenciales consecuencias son la exposición de información y/o obtención de privilegios.

Productos Afectados

FortiAnalyzer desde la versión 6.2.0 hasta la 6.2.3, la 6.0.8 y anteriores.
FortiManager desde la versión 6.2.0 hasta la 6.2.3, 6.0.8 y anteriores.
FortiAP-S/W2 versión 6.2.3 y anteriores.
FortiAP-U versión 6.0.1 y anteriores.

Mitigaciones

FortiAnalyzer: Actualizar a la versión 6.0.9, 6.2.4 o superior.
FortiManager: Actualizar a la versión 6.0.9, 6.2.4 o superior.
FortiAP-S/W2: Actualizar a la versión 6.2.4 o superior.
FortiAP-U: Actualizar a la versión 6.0.2 o superior.

Enlaces

https://fortiguard.com/psirt/FG-IR-19-292
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1653

CVE-2019-17655

Una vulnerabilidad de almacenamiento en texto plano de un archivo (CWE-313) en FortiOS SSL VPN podría permitir a un atacante obtener las credenciales de un usuario conectado con SSL VPN almacenadas en el sistema que se atacará. Para una explotación exitosa, se requeriría primero explotar otra vulnerabilidad, por ejemplo, filtración de información.

Productos Afectados

FortiOS desde la versión 6.2.0 hasta la 6.2.2, 6.0.9 y anteriores.

Mitigaciones

Actualizar a la versión 6.0.10, 6.2.3 o superior de FortiOS.

Enlaces

https://fortiguard.com/psirt/FG-IR-19-217
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17655

CVE-2019-9193

Una vulnerabilidad de tipo inyección de comandos de Sistema Operativo en FortiManager y FortiAnalyzer podrían permitir a un administrador privilegiado ejecutar estos comandos en el sistema a través de la inyección de consultas SQL.

Productos Afectados

FortiAnalyzer desde la versión 6.2.0 hasta la 6.2.3, 6.0.8 y anteriores.
FortiManager desde la versión 6.2.0 hasta la 6.2.3, 6.0.8 y anteriores.

Mitigaciones

FortiAnalyzer Actualizar a la versión 6.0.9, 6.2.4 o superior.
FortiManager Actualizar a la versión 6.0.9, 6.2.4 o superior.

Enlaces

https://fortiguard.com/psirt/FG-IR-19-294
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9193

CVE-2019-6693

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 versiones 6.2.0, 6.0.0 - 6.0.6, 5.6.10 y anteriores.
(Afecta a todos los datos de credenciales de tipo «ENC» en la configuración de FortiOS CLI, excepto a la contraseña del administrador).

Mitigaciones

En las versiones 5.6.11, 6.0.7, 6.2.1 y superiores, los administradores pueden elegir solicitar una clave, la cual luego es utiliza por FortiOS para desencriptar datos sensibles en el archivo de configuración. Los pasos para activar esta opción son los siguientes:

config system global
set private-data-encryption enable / desactivado por defecto */*
end

Enlaces

https://fortiguard.com/psirt/FG-IR-19-007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6693

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.
FortiAnalyzer versión 6.2.3 y anteriores.
(Afecta a todos los datos de credenciales de tipo «ENC» en la configuración CLI).

Mitigaciones

Los administradores pueden elegir solicitar una clave, la cual luego es utiliza por FortiManager o FortiAnalyzer para desencriptar datos sensibles en el archivo de configuración. Los pasos para activar esta opción son los siguientes:

config system global
set private-data-encryption enable / desactivado 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-2020-12812

Una vulnerabilidad de tipo autenticación inapropiada en SSL VPN de FortiOS podría resultar en que un usuario logre acceder a su cuenta sin validar el segundo factor de autenticación (FortiToken) si cambian de mayúscula a minúscula o viceversa el nombre de usuario. Esto pasa cuando el segundo factor de autenticación es activado en la configuración de "usuario local" y que la autenticación de usuario está configurada con el método de autenticación remota (por ejemplo, LDAP).

Productos Afectados

FortiOS versiones 6.4.0, 6.2.0 - 6.2.3, 6.0.9 y anteriores.

Mitigaciones

Actualizar a una de las siguientes versiones de FortiOS:
6.4.1 o superior.
6.2.4 o superior.
6.0.10 o superior.

Enlaces

https://fortiguard.com/psirt/FG-IR-19-283
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12812