Alerta de seguridad cibernética	9VSA21-00355-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de enero de 2021
Última revisión	07 de enero de 2021

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 entregada por Fortinet sobre una serie de vulnerabilidades que afectan a varios de sus productos.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2020-29010
CVE-2020-29016
CVE-2020-29017
CVE-2020-29018
CVE-2020-29019

CVE-2020-29010

Esta vulnerabilidad es categorizada como de riesgo medio, ya que permite a un usuario remoto ganar acceso a información potencialmente sensibe al leer los logs SSL VPN de otros usuarios.

Productos Afectados
FortiGate, versiones 6.0.0 a la 6.4.1.

Mitigación
Instalar las actualizaciones desde el sitio del proveedor.

Enlaces
https://www.fortiguard.com/psirt/FG-IR-20-103

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29010

CVE-2020-29016

Esta vulnerabilidad es categorizada como de riesgo alto, ya que permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. La vulnerabilidad existe debido a un error al procesar solicitudes HTTP.

Productos Afectados
FortiWeb, versiones 6.2.0 a la 6.3.5.

Mitigación
Instalar las actualizaciones desde el sitio del proveedor.

Enlaces
https://www.fortiguard.com/psirt/FG-IR-20-125

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29016

CVE-2020-29017

Esta vulnerabilidad es categorizada como de riesgo medio, ya que permite a un usuario remoto ejecutar comandos shell en el sistema objetivo.

Productos Afectados
FortiDeceptor, versiones 3.0.0, 3.0.1 y 3.1.0.

Mitigación
Instalar las actualizaciones desde el sitio del proveedor.

Enlaces
https://www.fortiguard.com/psirt/FG-IR-20-177

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29017

CVE-2020-29018

Esta vulnerabilidad es categorizada como de riesgo medio, ya que un error de cadena de formato posibilita a un usuario remoto acceder a información sensible a través del parámetro “redir”.

Productos Afectados
FortiWeb, versiones 6.3.0 a la 6.3.5.

Mitigación
Instalar las actualizaciones desde el sitio del proveedor.

Enlaces
https://www.fortiguard.com/psirt/FG-IR-20-123

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29018

CVE-2020-29019

Esta vulnerabilidad es categorizada como de riesgo medio, ya que permite a un usuario remoto no autenticado realizar un ataque de denegación de servicio (DoS).

Productos Afectados

FortiWeb, versiones de la 6.2.0 a la 6.3.7.

Mitigación

Instalar las actualizaciones desde el sitio del proveedor.

Enlaces

https://www.fortiguard.com/psirt/%20FG-IR-20-126

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29019