Alerta de seguridad cibernética	9VSA21-00386-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	8 de febrero de 2021
Última revisión	8 de febrero 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 de Gobierno, comparte la información entregada por Fortinet sobre vulnerabilidades críticas que afectan a sus productos Fortiweb y FortiDeceptor.

Este informe incluye las medidas de mitigación, consistentes en instalar las actualizaciones de los productos afectados cuando estén disponibles.

Vulnerabilidad

CVE-2021-21465
CVE-2020-29016
CVE-2020-29017
CVE-2020-29018

Impacto

CVE-2021-21465: Esta vulnerabilidad aprovecha una sanitización insuficiente de los datos ingresados por el usuario y que pasan a través de la cabecera Authorization. Un atacante remoto no autenticado puede enviar una solicitud especialmente diseñada a la aplicación afectada y ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación. La explotación exitosa de esta vulnerabilidad puede permitir a un atacante remoto leer, borrar y modificar la base de datos de la aplicación afectada.

CVE-2020-29016: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. La vulnerabilidad existe debido a un error al procesar solicitudes HTTP.

CVE-2020-29017: Esta vulnerabilidad aprovecha un error en la validación de entradas en la página de personalizadión de FortiDeceptor, por lo que permite a un usuario remoto ejecutar comandos shell en el sistema objetivo.

CVE-2020-29018: Esta vulnerabilidad existe debido a que un error de cadena de formato posibilita a un usuario remoto acceder a información sensible a través del parámetro “redir”.

Productos Afectados

Fortinet FortiWeb versiones 6.3.7 y anteriores.
Fortinet FortiDeceptor versiones 3.1.0 y anteriores.

Mitigación

Instalar las respectivas actualizaciones desde el sitio del proveedor.

Enlaces

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

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

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21465

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

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

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