Alerta de seguridad informática	9VSA20-00227-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2020
Última revisión	27 de mayo 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 dos vulnerabilidades que afectan sus productos FortiGateCloud y FortiClient. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-9291
CWE-79

CVE-2020-9291

Un atacante local podría escalar privilegios en el sistema afectado, mediante el agotamiento de nombres de archivos temporales combinado con un ataque de enlace simbólico.

Productos Afectados
FortiClient para Windows versión 6.2.1 y anteriores.

Mitigación
Actualizar a la versión 6.2.2 o superior de FortiClient para Windows.

Enlaces
https://fortiguard.com/psirt/FG-IR-20-040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9291

CWE-79

Debido a una inapropiada neutralización de datos ingresados por el usuario en la página de autenticación, un atacante remoto y sin autenticación podría realizar un ataque Reflected XSS (comandos en sitios cruzados reflejado) a través de una petición de autenticación especialmente diseñada, permitiéndole acceder a información potencialmente sensible en el sistema afectado.

Productos Afectados
FortiGateCloud versión 4.4.

Mitigación
Corregido en la versión 20.1 (desde el año 2020, este producto ocupará una nueva sintaxis para las versiones).

Enlaces
https://fortiguard.com/psirt/FG-IR-19-306
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13435