Alerta de seguridad informática	9VSA-00090-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de noviembre de 2019
Última revisión	25 de noviembre de 2019

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 información obtenida del sitio oficial de FortiGuard referente a una vulnerabilidad que afecta a su herramienta de monitoreo DHCP, la cual, si es explotada, puede resultar en ataques remotos de tipo XSS persistente (Stored Cross-site Scripting). El informe contiene información sobre las actualizaciones para mitigar el riesgo.

Vulnerabilidad

CVE-2019-6697

Impacto

El monitor DHCP de FortiGuard permite generar ataques XSS con persistencia.
Este ataque es posible por la falta de sanitización en el parámetro Hostname, entregado por el usuario, a través de los paquetes DHCP.
Un atacante en la misma red del sistema, sin autenticación, podría enviar paquetes DHCP especialmente diseñados para ejecutar código HTML y script en el browser del administrador. Una explotación exitosa permitiría al atacante robar información potencialmente sensible, cambiar la apariencia del sitio en el browser, generar ataques phishing y hasta descargar malware.

Productos Afectados

FortiGate versiones:
6.0.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4, 6.0.5, 6.0.6.
6.2.0, 6.2.1.

Mitigaciones

Se debe actualizar a las versiones de FortiGate 6.0.7, 6.2.2 o superiores.

Enlaces

https://fortiguard.com/psirt/%20FG-IR-19-184
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-6697