Alerta de seguridad informática	9VSA-00091-001
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 McAfee referente a una vulnerabilidad que afecta a su herramienta McAfee Client Proxy (MCP) en el sistema operativo Windows, la cual, si es explotada, puede resultar en la evasión local de autenticación. Este informe incluye la respectiva actualización para mitigar el riesgo.

Vulnerabilidad

CVE-2019-3654

Impacto

Una vulnerabilidad de tipo escalación de privilegios puede permitir a un atacante generar códigos de autorización en la máquina cliente (éstos solamente deben ser generados por un administrador), permitiendo al atacante visitar sitios bloqueados por MWG (McAfee Web Gateway) por un periodo corto de tiempo.
La explotación es aparentemente difícil, y requiere que el atacante esté autenticado en la red local. El atacante debe modificar un archivo de código del cliente Windows para generar estos códigos de autorización.

Productos Afectados

Todas las versiones 2.x de McAfee Client Proxy (MCP).

Mitigaciones

Se debe actualizar a la versión 3.0.0 de McAfee Client Proxy (MCP).
Instrucciones de actualización y descarga:
https://kc.mcafee.com/corporate/index?page=content&id=KB56057

Enlaces

https://kc.mcafee.com/corporate/index?page=content&id=SB10305
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-3654