

Alerta de seguridad informática	9VSA-00072-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de octubre de 2019
Última revisión	21 de octubre 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 la información entregada por Fortiguard Labs correspondiente a dos vulnerabilidades que afectan a FortiMail.

Vulnerabilidad

CVE-2019-15712

CVE-2019-15707

Impacto

Dos vulnerabilidades inadecuadas de control de acceso en FortiMail admin webUI pueden permitir a los administradores realizar funciones privilegiadas para las que no deberían estar autorizados.

CVE-2019-15712: control de acceso incorrecto a la consola web

CVE-2019-15707: control de acceso incorrecto a la descarga de la configuración de respaldo del sistema

Productos Afectados

FortiMail 6.2.0, 6.0.0 a 6.0.6, 5.4.10 y anteriores.

Mitigación

Aplicar las actualizaciones a las versiones 6.2.1, 6.0.7 o 5.4.11 publicadas por el fabricante según corresponda.

Enlace

<https://fortiguard.com/psirt/FG-IR-19-237>