Alerta de seguridad informática	9VSA-00049-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de septiembre de 2019
Última revisión	12 de septiembre 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 obtenida de diferentes fuentes, referente a vulnerabilidades detectadas en el agente de transferencia de correos EXIM para Linux, junto a su respectiva actualización para mitigar el riesgo.

Vulnerabilidad

- CVE-2019-15846

Impacto

- La vulnerabilidad solo afecta a servidores que acepten conexiones TLS tras recibir el final de “SNI” en una secuencia “backslack-null” en la negociación inicial de la conexión cifrada. Esto causa un “buffer overflow” en el proceso de envío de SMTP, permitiendo al atacante inyectar código malicioso que EXIM ejecutaría como root.

Productos Afectados

Todas las versiones entre la 4.80 hasta la 4.92.1.
(Las versiones anteriores a la 4.80, si bien no están expuestas al CVE-2019-15846, se encuentran expuestas a otra vulnerabilidad crítica, CVE-2018-6789)

Mitigación

Actualizar a la versión de EXIM 4.92.2

Enlaces

- https://nvd.nist.gov/vuln/detail/CVE-2019-15846
- https://www.tenable.com/cve/CVE-2019-15846
- https://shieldnow.co/2019/09/06/vulnerabilidad-critica-de-servidor-tls-en-exim-cve-2019-15846/

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.09.12 10:25:40 -03'00'