Alerta de seguridad informática	**9VSA-00057-001**
Clase de alerta	**Vulnerabilidad**
Tipo de incidente	**Sistema y/o Software Abierto**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**01 de octubre de 2019**
Última revisión	**01 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 obtenida del sitio web de EXIM, referente a una vulnerabilidad detectada en el agente de transferencia de correos EXIM para Linux, junto a su respectiva actualización para mitigar el riesgo.

Vulnerabilidad

- CVE-2019-16928

Impacto

Esta vulnerabilidad puede ser gatillada utilizando el desbordamiento del buffer basado en string_vformat (string.c). El exploit utiliza una cadena EHLO extraordinariamente larga para realizar un ataque de denegación de servicios o posible ejecución de código remoto. Si bien, en el momento de recibir los mensajes Exim ya no está con privilegios, se podrían utilizar otros caminos para obtenerlos.

Productos Afectados

Todas las versiones entre la 4.92 hasta la 4.92.2 (incluidas ambas).

Mitigación

Actualizar a la versión de EXIM 4.92.3

Enlaces

- https://nvd.nist.gov/vuln/detail/CVE-2019-16928
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16928
- https://www.exim.org/static/doc/security/CVE-2019-16928.txt

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.01 14:47:19 -03'00'