# Vulnerabilidad en servidores Exim permite ataques de ejecución de código remotos

Autor: I. Stepanenko

Fecha: Saturday 21st of September 2019 05:22:57 AM

Se descubrió una vulnerabilidad crítica de ejecución remota de código en el popular software de servidor de correo electrónico Exim de código abierto, que deja al menos más de medio millón de servidores de correo electrónico vulnerables a los piratas informáticos remotos.

Los mantenedores de Exim lanzaron hoy la versión 4.92.2 de Exim luego de publicar una advertencia temprana hace dos días, dando a los administradores del sistema un aviso de sus próximos parches de seguridad que afectan a todas las versiones del software del servidor de correo electrónico hasta la última versión 4.92.1.

Exim es un software de agente de transferencia de código abierto (MTA) ampliamente utilizado desarrollado para sistemas operativos tipo Unix, como Linux, Mac OSX o Solaris, que actualmente ejecuta casi el 60% de los servidores de correo electrónico de Internet para enrutar, entregar y recibir mensajes de correo.

La vulnerabilidad identificada como CVE-2019-15846, solo afecta a los servidores Exim que aceptan conexiones TLS, lo que potencialmente permite a los atacantes obtener acceso de nivel raíz al sistema *“al enviar un SNI que termina en una secuencia de barra invertida*

*durante el apretón de manos TLS inicial".*

SNI, que significa Indicación de Nombre del Servidor, es una extensión del protocolo TLS que permite que el servidor aloje de forma segura múltiples certificados TLS para distintos sitios, todo bajo una sola dirección IP.

Según el equipo de Exim, dado que la vulnerabilidad no depende de la biblioteca TLS utilizada por el servidor, GnuTLS y OpenSSL se ven afectados.

Además, aunque la configuración predeterminada del software del servidor de correo Exim no viene con TLS habilitado, algunos sistemas operativos incluyen el software Exim con la función vulnerables habilitada de forma predeterminada.

La vulnerabilidad fue descubierta por un colaborador de código abierto e investigador de seguridad que utiliza el alias en línea Zerons y analizada por expertos en seguridad cibernética de Qualys.

Hace tres meses, Exim también parchó una grave vulnerabilidad de ejecución remota de comandos, rastreada como CVE-2019-10149, que fue explotada activamente en la naturaleza por varios grupos de hackers para comprometer servidores vulnerables.

El aviso de Exim dice que existe una prueba de concepto (PoC) rudimentaria para este defecto, pero actualmente no existe ningún exploit disponible para el público.

Se recomienda a los administradores de servidores que instalen la última versión de Exim 4.92.2 de inmediato, y de no ser posible, mitigar el programa al no permitir que los servidores Exim sin parches acepten conexiones TLS.