Se ha descubierto y corregido una vulnerabilidad de seguridad crítica en el popular software de servidor de correo electrónico Exim de código abierto, que podría permitir que un hacker remoto bloquee o ejecute potencialmente código malicioso en los servidores de destino.

Los mantenedores de Exim lanzaron hoy una actualización de seguridad urgente, Exim versión 4.92.3, luego de publicar una advertencia temprana hace dos días, dando a los administradores del sistema un adelanto anticipado de sus próximos parches de seguridad que afectan a todas las versiones del software del servidor de correo electrónico desde 4.92 hasta e incluyendo la última versión 4.92.2.

Exim es un agente de transferencia de correo 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 electrónico.

Esta es la segunda vez en este mes cuando los encargados de Exim lanzaron una actualización de seguridad urgente. A inicios de este mes, el equipo parchó un error crítico de ejecución remota de código (CVE-2019-15846), en el software que podría haber permitido a los atacantes remotos obtener acceso de nivel raíz al sistema.

Identificada como CVE-2019-16928 y descubierta por Jeremy Harris del equipo de desarrollo Exim, la vulnerabilidad es un problema de desbordamiento de búfer (corrupción de memoria) basado en string_vformat, definido en el archivo string.c del componente EHLO Command Handler.

La falla de seguridad podría permitir a los atacantes remotos causar una condición de denegación de servicio (DoS) o ejecutar código arbitrario en un servidor de correo Exim específico utilizando una línea especialmente diseñada en el comando EHLO con los derechos del usuario objetivo.

Según el aviso de Exim, un exploit de PoC actualmente conocido para esta vulnerabilidad

permite bloquear el proceso Exim enviando una cadena larga en el comando EHLO, aunque otros comandos también podrían usarse para ejecutar potencialmente código arbitrario.

> *«El exploit actualmente conocido utiliza una cadena EHLO larga extraordinaria para bloquear el proceso de Exim que está recibiendo el mensaje. Mientras que en este modo de operación, Exim ya perdió sus privilegios, pueden existir otras rutas para llegar al código vulnerable»,* dice el equipo de desarrolladores de Exim.

A mediados de año, Exim también parchó una grave vulnerabilidad de ejecución remota de comandos (CVE-2019-10149) en su software de correo electrónico que fue explotada activamente en la naturaleza por distintos grupos de hackers para comprometer servidores vulnerables.

Por lo tanto, se recomienda a los administradores de servidor que instalen la última versión de Exim 4.92.3 lo antes posible, ya que no existe una mitigación conocida para resolver este problema temporalmente.

El equipo también dijo *«si no puede instalar las versiones anteriores, solicite a su responsable de paquetes una versión que contenga la solución respaldada. A pedido y dependiendo de nuestros recursos, le ayudaremos a respaldar la solución».*

La actualización de seguridad está disponible para distribuciones de Linux, incluyendo Ubuntu, Arch Linux, FreeBSD, Debian y Fedora.