Se han revelado múltiples vulnerabilidades de seguridad en el agente de transferencia de correo Exim, que, si se explotan con éxito, podrían dar lugar a la divulgación de información y la ejecución remota de código.

La lista de fallos, que fueron reportados de forma anónima en junio de 2022, es la siguiente:

- CVE-2023-42114 (puntuación CVSS: 3.7) – Vulnerabilidad de divulgación de información por lectura fuera de límites en Exim NTLM Challenge.
- CVE-2023-42115 (puntuación CVSS: 9.8) – Vulnerabilidad de ejecución remota de código por escritura fuera de límites en Exim AUTH.
- CVE-2023-42116 (puntuación CVSS: 8.1) – Vulnerabilidad de desbordamiento de búfer en la pila en Exim SMTP Challenge que permite la ejecución remota de código.
- CVE-2023-42117 (puntuación CVSS: 8.1) – Vulnerabilidad de ejecución remota de código por neutralización incorrecta de elementos especiales en Exim.
- CVE-2023-42118 (puntuación CVSS: 7.5) – Vulnerabilidad de ejecución remota de código por subflujo de enteros en Exim libspf2.
- CVE-2023-42119 (puntuación CVSS: 3.1) – Vulnerabilidad de divulgación de información por lectura fuera de límites en Exim dnsdb.

La vulnerabilidad más crítica es CVE-2023-42115, que permite a atacantes remotos no autenticados ejecutar código arbitrario en instalaciones de Exim afectadas.

> *«El problema específico reside en el servicio SMTP, que escucha en el puerto TCP 25 de forma predeterminada»*, advirtió Zero Day Initiative en un comunicado publicado esta semana.

> *«Este problema se debe a la falta de validación adecuada de los datos proporcionados por el usuario, lo que puede resultar en una escritura más allá del final de un búfer. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto de la cuenta de servicio».*

Los mantenedores de Exim, en un mensaje compartido en la lista de correo de seguridad de código abierto (oss-security), indicaron que las correcciones para CVE-2023-42114, CVE-2023-42115 y CVE-2023-42116 están *«disponibles en un repositorio protegido y están listas para ser aplicadas por los mantenedores de la distribución».*

«Los problemas restantes son debatibles o carecen de información que necesitamos para solucionarlos», agregaron, mencionando que solicitaron más detalles a ZDI sobre los problemas y que no recibieron respuestas con las que pudieran trabajar hasta mayo de 2023. El equipo de Exim también señaló que están a la espera de obtener detalles precisos sobre las otras tres deficiencias.

Sin embargo, ZDI se defendió de las afirmaciones de un *«manejo descuidado»* y de que *«ninguno de los equipos se comunicó con el otro durante 10 meses»*, indicando que se pusieron en contacto varias veces con los desarrolladores.

> *«Después de que se superó ampliamente nuestra línea de tiempo de divulgación en muchos meses, notificamos al responsable de nuestra intención de hacer públicos estos errores, momento en el que se nos dijo: 'hagan lo que tengan que hacer'»*, explicaron.

> *«Si estos errores han sido abordados adecuadamente, actualizaremos nuestras advertencias con un enlace a la advertencia de seguridad, la inclusión de código o cualquier otra documentación pública que cierre el problema».*

Ante la falta de parches, ZDI recomienda restringir la interacción con la aplicación como la única estrategia de mitigación *«significativa».*

No es la primera vez que se descubren fallas de seguridad en el ampliamente utilizado agente de transferencia de correo. En mayo de 2021, Qualys reveló un conjunto de 21

vulnerabilidades agrupadas bajo el nombre de 21Nails que permiten a atacantes no autenticados lograr una ejecución remota de código completa y obtener privilegios de root.

Previamente, en mayo de 2020, el gobierno de Estados Unidos informó que hackers afiliados a Sandworm, un grupo respaldado por un estado de Rusia, habían estado explotando una vulnerabilidad crítica en Exim (CVE-2019-10149, puntuación CVSS: 9.8) para infiltrar redes sensibles.

Este desarrollo también se produce poco después de un nuevo estudio realizado por investigadores de la Universidad de California en San Diego, que descubrió una técnica novedosa llamada *«spoofing basado en reenvío»* que aprovecha debilidades en el reenvío de correo electrónico para enviar mensajes que se hacen pasar por entidades legítimas, comprometiendo así la integridad.

> *«El protocolo original utilizado para verificar la autenticidad de un correo electrónico parte de la suposición implícita de que cada organización administra su propia infraestructura de correo, con direcciones IP específicas que no son compartidas por otros dominios»,* dijeron los investigadores.

> *«Sin embargo, en la actualidad, muchas organizaciones subcontratan su infraestructura de correo electrónico a servicios como Gmail y Outlook. Como resultado, miles de dominios han otorgado el permiso para enviar correos electrónicos en su nombre al mismo tercero. Aunque estos proveedores de terceros verifican que sus usuarios solo envíen correos en nombre de los dominios que administran, esta protección puede ser eludida mediante el reenvío de correos electrónicos.»*