BOLETÍN DE ALERTA

Boletín Nro.: 2023-48
Fecha de publicación: 03/10/2023
Tema: Múltiples Vulnerabilidades Críticas para Exim

Productos afectados:

- Exim v4.96
- libspf2.

Descripción:

Se han descubierto cuatro vulnerabilidades en el software Exim v4.96 y la librería libspf2, tres de las cuales son de severidad alta y una es crítica. Las vulnerabilidades permiten a un atacante remoto ejecutar código arbitrario en las instalaciones afectadas de Exim.

La vulnerabilidad crítica, identificada como CVE-2023-42115, se debe a la falta de una validación adecuada de los datos proporcionados por el usuario en el servicio SMTP, lo que puede provocar una escritura más allá del final de un búfer. Un atacante podría aprovechar esta vulnerabilidad para ejecutar código en el contexto de la cuenta de servicio. La única solución recomendada para esta vulnerabilidad es restringir la interacción con la aplicación.

Las vulnerabilidades CVE-2023-42117 y CVE-2023-42118, que consisten en no utilizar Exim detrás de un proxy-protocolo no fiable y no utilizar la condición "spf" en su ACL.

Las vulnerabilidades CVE-2023-42115 y CVE-2023-42116 se han solucionado en las versiones 4.96.1 y 4.97, y las correcciones están disponibles en un repositorio protegido para ser aplicadas por los mantenedores de la distribución.

Impacto:

Un atacante remoto podría aprovechar estas vulnerabilidades para ejecutar código arbitrario y comprometer la seguridad de la red de la organización afectada.

Solución:

Se recomienda a los usuarios de Exim que actualicen a las versiones 4.96.1 o 4.97 para solucionar las vulnerabilidades CVE-2023-42115 y CVE-2023-42116. Para las vulnerabilidades CVE-2023-42117 y CVE-2023-42118, se recomienda no utilizar Exim detrás de un proxy-protocolo no fiable y no utilizar la condición "spf" en su ACL para mitigar el riesgo. En el caso de la vulnerabilidad crítica, la única solución recomendada es restringir la interacción con la aplicación.

Información adicional:

- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-exim?sstc=u21488nl264934
- https://www.zerodayinitiative.com/advisories/ZDI-23-1469/
- https://www.zerodayinitiative.com/advisories/ZDI-23-1470/
- https://www.zerodayinitiative.com/advisories/ZDI-23-1471/
- https://www.zerodayinitiative.com/advisories/ZDI-23-1472/
- https://seclists.org/oss-sec/2023/q3/254
- https://exim.org/static/doc/security/CVE-2023-zdi.txt
- https://exim.org/download.html