El «hotpatch» lanzado por Amazon Web Services (AWS) en respuesta a las vulnerabilidades de Log4Shell, podría aprovecharse para el escape de contenedores y la escalada de privilegios, lo que permite a un atacante tomar el control del host subyacente.

> *«Además de los contenedores, los procesos sin privilegios también pueden explotar el parche para aumentar los privilegios y obtener la ejecución del código raíz»,* dijo el investigador de Unit 42 de Palo Alto Networks, Yuval Avrahami.

Las vulnerabilidades, CVE-2021-3100, CVE-2021-3101, CVE-2022-0070 y CVE-2022-0071 (puntajes CVSS: 8.8), afectan a las soluciones de revisión enviadas por AWS y se derivan del hecho de que son diseñados para buscar procesos de Java y parchearlos contra la falla de Log4j sobre la marcha, pero sin garantizar que los nuevos procesos de Java se ejecuten dentro de las restricciones impuestas en el contenedor.

> *«Cualquier proceso que ejecute un binario llamado 'java' dentro o fuera de un contenedor, se considera candidato para la zona activa. Por lo tanto, un contenedor malicioso podría haber incluido un binario malicioso llamado 'java' para engañar a la solución de parche caliente instalada para que la invoque con privilegios elevados»,* explicó Avrahami.

En el paso siguiente, los privilegios elevados podrían ser armados por el proceso malicioso 'java' para escapar del contenedor y obtener el control total sobre el servidor comprometido.

Un proceso no autorizado sin privilegios, de forma similar, podría haber creado y ejecutado un binario malicioso llamado «java» para engañar al servicio hotpatch para que lo ejecute con privilegios elevados.

Se recomienda a los usuarios que actualicen a la versión de revisión activa lo más pronto

posible para evitar una posible explotación, pero solo después de priorizar la aplicación de parches contra las fallas de Log4Shell explotadas activamente.

> *«Los contenedores por lo general se usan como un límite de seguridad entre las aplicaciones que se ejecutan en la misma máquina. Un escape de contenedor permite a un atacante extender una campaña más allá de una sola aplicación y comprometer los servicios vecinos»,* dijo Avrahami.