Jenkins, el popular software de servidor de automatización de código abierto, publicó un aviso el lunes sobre una vulnerabilidad crítica en el servidor web Jetty, que podría dañar la memoria y hacer que se divulgue información confidencial.

Rastreada como CVE-2019-17638, la vulnerabilidad tiene una clasificación CVSS de 9.4, e impacta en las versiones 9.4.27v20200227 a 9.4.29.v20200521 de Eclipse Jetty, una herramienta con todas las funciones que proporciona un servidor HTTP Java y un contenedor web para su uso en marcos de software.

> *«Jenkins incluye Winstone-Jetty, un envoltorio de Jetty, para que actúe como servidor HTTP y Servlet cuando se comienza a usar java -jar jenkins.war. Así es como se ejecuta Jenkins cuando se utiliza cualquiera de los instaladores o paquetes, pero no cuando se ejecuta con contenedores servlet como Tomcat»,* dice el aviso.
>
> *«La vulnerabilidad puede permitir que atacantes no autenticados obtengan encabezados de respuesta HTTP que pueden incluir datos confidenciales destinados a otro usuario».*

La falla, que afecta a Jetty y Jenkins Core, parece haber sido introducida en la versión 9.4.27 de Jetty, que agregó un mecanismo para manejar grandes encabezados de respuesta HTTP y evitar desbordamientos de búfer.

> *«El problema fue en el caso de un desbordamiento del búfer, liberamos el búfer del encabezado, pero no anulamos el campo»,* dijo el jefe del proyecto de Jetty, Greg Wilkins.

Para manejar esto, Jetty lanza una excepción para producir un error HTTP 431, lo que hace que los encabezados de respuesta HTTP se publiquen en el grupo de búfer dos veces, lo que

a su vez provoca daños en la memoria y divulgación de información.

Por lo tanto, debido a la doble liberación, dos subprocesos pueden adquirir el mismo búfer del grupo al mismo tiempo y potencialmente permitir que una solicitud acceda a una respuesta escrita por el otro subproceso, que puede incluir identificadores de sesión, credenciales de autenticación y otra información confidencial.

> *«Mientras que thread1 está a punto de usar ByteBuffer para escribir datos de response1, thread2 llena el ByteBuffer con datos de response2. Thread1 luego procede a escribir el búfer que ahora contiene datos de response2. Esto da como resultado client1, que emitió request1 y espera respuestas, para ver response2 que podría contener datos confidenciales pertenecientes a client2».*

En un caso, la corrupción de la memoria hizo posible que los clientes se movieran entre sesiones, por lo que tenían acceso entre cuentas, ya que las cookies de autenticación de la respuesta de un usuario se enviaban a otro usuario, lo que permitía al usuario A saltar a la sesión del usuario B.

Después de revelarse las implicaciones de seguridad, la vulnerabilidad se abordó en Jetty 9.4.30v20200611 lanzado el mes pasado. Jenkins Winstone corrigió la falla en su utilidad en Jenkins 2.243 y Jenkins LTS 2.235.5 lanzados ayer.