Se revelaron dos vulnerabilidades de seguridad graves en el servidor de automatización de código abierto Jenkins, que podrían conducir a la ejecución de código en sistemas específicos.

Las vulnerabilidades, rastreadas como CVE-2023-27898 y CVE-2023-27905, afectan al servidor Jenkins y el Centro de Actualización, y han sido nombradas de forma colectiva como CorePlague por la compañía de seguridad en la nube Aqua. Todas las versiones de Jenkins anteriores a la 2.319.2 son vulnerables y explotables.

> *«Explotar estas vulnerabilidades podría permitir que un atacante no autenticado ejecute código arbitrario en el servidor Jenkins de la víctima, lo que podría llevar a un compromiso completo del servidor Jenkins»*, dijo la compañía en un informe.

Las deficiencias son el resultado de cómo Jenkins procesa los complementos disponibles en el Centro de Actualizaciones, lo que permite potencialmente que un hacker cargue un complemento con una carga maliciosa y desencadene un ataque de secuencias de comandos entre sitios (XSS).

> *«Una vez que la víctima abre el 'Administrador de complementos disponibles' en su servidor Jenkins, se activa el XSS, lo que permite a los atacantes ejecutar código arbitrario en el servidor usando la API de la consola de scripts»,* dijo Aqua.

Debido a que también es un caso de XSS almacenado en el que el código JavaScript se inyecta en el servidor, la vulnerabilidad se puede activar sin tener que instalar el complemento o incluso visitar la URL del complemento en primer lugar.

De forma preocupante, las vulnerabilidades también podrían afectar a los servidores Jenkins autohospedados y ser explotados incluso en escenarios en los que el servidor no es accesible públicamente a través de Internet, ya que los atacantes podrían *«inyectar el Centro de actualización público de Jenkins».*

Sin embargo, el ataque se basa en el requisito previo de que el complemento falso sea compatible con el servidor Jenkins y aparezca en la parte superior de la fuente principal en la página *«Administrador de complementos disponibles».*

Según Aqua, esto puede manipularse *«cargando un complemento que contenga todos los nombres de complementos y palabras clave populares incrustadas en la descripción»*, o aumentar artificialmente el recuento de descargas del complemento mediante el envío de solicitudes de instancias falsas.

Después de la divulgación responsable el 24 de enero de 2023, Jenkins lanzó parches para el Centro de actualizaciones y el servidor. Se recomienda a los usuarios que actualicen su servidor Jenkins a la última versión disponible para mitigar los riesgos potenciales.