Una vulnerabilidad de seguridad crítica fue revelada en el framework Quarkus Java, que podría explotarse potencialmente para lograr la ejecución remota de código en los sistema afectados.

Rastreada como CVE-2022-4116 (puntaje CVSS: 9.8), la vulnerabilidad podría ser abusada trivialmente por un hacker sin ningún privilegio.

> *«La vulnerabilidad se encuentra en Dev UI Config Editor, que es vulnerable a ataques de host local que podrían conducir a la ejecución remota de código (RCE)»,* dijo el investigador de Contrast Security, Joseph Beeton, quién informó el error.

Quarkus, desarrollado por Red Hat, es un proyecto de código abierto que se utiliza para crear aplicaciones Java en entornos en contenedores y sin servidor.

Cabe mencionar que el problema solo afecta a los desarrolladores que ejecutan Quarkus y son engañados par que visiten un sitio web especialmente diseñado, que está incrustado con un código JavaScript malicioso diseñado para instalar o ejecutar cargas útiles arbitrarias.

Esto podría tomar la forma de un ataque de spear-phishing de un pozo de agua sin requerir ninguna interacción adicional por parte de la víctima. Alternativamente, el ataque se puede realizar mediante la publicación de anuncios maliciosos en sitios web populares frecuentados por desarrolladores.

La interfaz de usuario de desarrollo, que se ofrece por medio de un modo de desarrollo, está vinculada a localhost y permite a un desarrollador monitorear el estado de una aplicación, cambiar la configuración, migrar bases de datos y borrar cachés.

Debido a que está restringida a la máquina local del desarrollador, la interfaz de usuario de Dev también carece de controles de seguridad cruciales como la autenticación y el uso compartido de recursos de origen cruzado (CORS) para evitar que un sitio web fraudulento lea ls datos de otro sitio.

El problema identificado por Contrast Security radica en el hecho de que el código JavaScript alojado en un sitio web con malware puede convertirse en un arma para modificar la configuración de la aplicación Quarkus a través de una solicitud HTTP POST para activar la ejecución del código.

> *«Si bien solo afecta al modo Dev, el impacto sigue siendo alto, ya que podría llevar a un atacante a obtener acceso local a su caja de desarrollo»,* dijo Quarkus en un aviso.

Se recomienda a los usuarios que actualicen a la versión 2.14.2.Final y 2.13.5.Final para protegerse contra la falla. Una posible solución es mover todos los puntos finales que no son de aplicación a una ruta raíz aleatoria.