Si estás utilizando la utilidad de administración de configuración de red rConfig para proteger y administrar tus dispositivos, debes tener en cuenta la siguiente advertencia de seguridad.

Un investigador de seguridad cibernética publicó recientemente detalles y exploits de prueba de concepto para dos vulnerabilidades de ejecución remota de código críticas y sin parches en la utilidad rConfig, una de estas podría permitir que atacantes remotos no autenticados comprometan servidores específicos y dispositivos de red conectados.

Escrito en PHP nativo, rConfig es una utilidad gratuita de gestión de configuración de dispositivos de red de código abierto que permite a los ingenieros de red la configuración y captura de pantalla de configuraciones frecuentes de sus dispositivos de red.

Según la página web del proyecto, rConfig se está utilizando para administrar más de 3.3 millones de dispositivos de red, incluidos conmutadores, enrutadores, cortafuegos, equilibradores de carga y optimizadores WAN.

Algo más preocupantes es que las dos vulnerabilidades afectan a todas las versiones de rConfig, incluida la última versión de rConfig 3.9.2, sin parche de seguridad disponible hasta este momento.

Mohammad Askar es quien descubrió las vulnerabilidades, y según sus informes, cada falla reside en un archivo separado de rConfig, la primera, identificada como CVE-2019-16662, puede explotarse remotamente sin requerir autenticación previa, mientras que la otra, CVE-2019-16663, requiere autenticación antes de su explotación.

En ambos casos, para explotar la falla, todo lo que un atacante debe hacer es acceder a los archivos vulnerables con un parámetro GET malformado diseñado para ejecutar comandos maliciosos del sistema operativo en el servidor de destino.

Las vulnerabilidades de PoC permiten a los atacantes obtener un shell remoto del servidor de la víctima, lo que les permite ejecutar cualquier comando arbitrario en el servidor comprometido con los mismos privilegios que la aplicación web.

Mientras tanto, otro investigador de seguridad independiente, analizó las vulnerabilidades y descubrió que la segunda vulnerabilidad RCE también podría ser explotada sin necesidad de autenticación en las versiones anteriores a la 3.6.0 de rConfig.

> *«Sin embargo, luego de revisar el código fuente de rConfig, descubrí que no solo rConfig 3.9.2 tiene esas vulnerabilidades, sino también todas sus versiones. Además, CVE-2019-16663, el RCE posterior a la autenticación puede explotarse sin autenticación para todas las versiones antes de rConfig 3.6.0»*, dijo el investigador.

Sin embargo, no todas las instalaciones de rConfig son vulnerables a la primera vulnerabilidad RCE pre autenticada, según informó el investigador de seguridad de SANS, Johannes Ullrich.

Luego de analizar las vulnerabilidades de día cero, Ulrrich descubrió que el archivo afectado asociado con la primera vulnerabilidad pertenece a un directorio requerido durante la instalación de rConfig en un servidor, que de lo contrario se eliminará después de la instalación.

En su sitio web, como parte de una lista de tareas esenciales que los usuarios deben seguir después de la instalación, rConfig también recomienda a los usuarios que *«eliminen el directorio de instalación después de que se complete la instalación».*

Esto quiere decir que los usuarios que eliminaron el directorio de instalación de rConfig como se recomienda, no son vulnerables a la primera falla de RCE, pero aún podrían estar en riesgo debido a la segunda falla RCE de impacto similar, que tampoco requiere autenticación para versiones anteriores como se explicó anteriormente.

En caso de que utilices rConfig, se recomienda eliminar temporalmente la aplicación del servidor o utilizar soluciones alternativas hasta que los parches de seguridad sean lanzados.