La compañía de infraestructura web y seguridad de sitios, Cloudflare, solucionó el mes pasado una vulnerabilidad crítica en su biblioteca CDNJS, que utiliza el 12.7% de todos los sitios web en Internet.

CDNJS es una red de distribución de contenido gratuita y de código abierto, que sirve alrededor de 4041 bibliotecas de JavaScript y CSS, lo que la convierte en la segunda CDN más popular para JavaScript luego de las bibliotecas alojadas de Google.

La debilidad se refería a un problema en el servidor de actualización de la biblioteca CDNJS que podría permitir a un atacante ejecutar comandos arbitrarios, lo que llevaría a un compromiso total.

La vulnerabilidad fue descubierta e informada por el investigador de seguridad RyotaK el 6 de abril de 2021. No existe evidencia de ataques en la naturaleza que abusen de la falla.

Específicamente, la vulnerabilidad funciona publicando paquetes en CDNJS de Cloudflare utilizando GitHub y npm, como medio para desencadenar una vulnerabilidad de recorrido de ruta, y en última instancia, engañar al servidor para que ejecute código arbitrario, logrando de este modo la ejecución remota de código.

Cabe mencionar que la infraestructura CDNJS incluye características para automatizar las actualizaciones de la biblioteca ejecutando de forma periódica scripts en el servidor para descargar archivos relevantes del respectivo repositorio de Git administrado por el usuario o del registro de paquetes npm.

Al descubrir un problema con la forma en que el mecanismo desinfecta las rutas de los paquetes, RyotaK descubrió que *«se puede ejecutar código arbitrario después de realizar un recorrido de ruta desde el archivo .tgz publicado en npm y sobrescribir el script que se ejecuta regularmente en el servidor».*

En otras palabras, el objetivo del ataque es publicar una nueva versión de un paquete especialmente diseñado en el repositorio, que luego se recoge en el servidor de actualización

de la biblioteca CDNJS para su publicación, en el proceso de copiar el contenido del paquete malicioso en un archivo de script ejecutado regularmente en el servidor, obteniendo así la ejecución de código arbitrario.

> *«Si bien esta vulnerabilidad podría explotarse sin ninguna habilidad especial, podría afectar a muchos sitios web. Debido a que existen muchas vulnerabilidades en la cadena de suministro, que son fáciles de explotar pero tienen un gran impacto, siendo que da mucho miedo»,* dijo RyotaK.

Esta no es la primera vez que el investigador de seguridad descubre fallas críticas en la forma en que se manejan las actualizaciones de los repositorios de software. En abril de 2021, RyotaK reveló una vulnerabilidad crítica en el repositorio oficial de Homebrew Cask, que podría haber sido aprovechada por un atacante para ejecutar código arbitrario en las máquinas de los usuarios.