El equipo detrás de NPM, el administrador de paquetes más grande para las bibliotecas de JavaScript, emitió ayer una alerta de seguridad, en la que aconseja a los usuarios que actualicen a la última versión 6.13.4, para evitar ataques de *«plantación binaria»*.

Los desarrolladores de NPM (Node.js Package Manager), dicen que el cliente de interfaz de línea de comandos (CLI) npm se ve afectado por un error de seguridad, una combinación entre un recorrido de archivo y un problema de escritura de archivo arbitrario.

Los atacantes podrían explotar el error para plantar binarios maliciosos o sobrescribir archivos en la computadora de un usuario.

La vulnerabilidad solo puede explotarse durante la instalación de un paquete npm boobytrapped por medio de la npm CLI.

«Sin embargo, como hemos visto en el pasado, esta no es una barrera insuperable», dijo el equipo de npm, refiriéndose a incidentes pasados en los que los atacantes planearon paquetes en el depósito oficial de npm.

Los desarrolladores de NPM afirman que han estado escaneando el portal npm en busca de paquetes que puedan contener código de explotación diseñado para aprovechar el error, pero no han encontrado nada sospechoso.

> *«Eso no garantiza que no se haya utilizado, pero si significa que actualmente no se está utilizando en paquetes publicados en el registro»*, dijeron los desarrolladores.
>
> *«Seguiremos monitoreando. Sin embargo, no podemos escanear todas las fuentes posibles de paquetes npm, por lo que es importante actualizar lo antes posible»,* agregaron.

Además de npm, yarn, otro administrador de paquetes para JavaScript, también se vio

afectado. El error se corrigió en el hilo con el lanzamiento del hilo 1.21.1, a inicios de la semana.

Los equipos de npm y yarn le dieron crédito al investigador de seguridad alemán, Daniel Ruf, por descubrir la vulnerabilidad. Un informe ténico en profundidad está disponible en el blog de Ruf.

Sin embargo, el problema afecta más a los usuarios de npm que a los hilos. NPM no solo es la aplicación de administración de paquetes más grande para JavaScript, sino que también es el repositorio de paquetes más grande para cualquier lenguaje de programación, con más de 350 mil bibliotecas.

Actualmente, JavaScript se ejecuta en todas partes, desde navegadores hasta aplicaciones financieras, desde escritorios hasta servidores. Esto debido a que npm tiene un papel tan central en el ecosistema de JavaScript, que a menudo se abusa de él.

Los hackers suben bibliotecas boobytrapped en npm con la esperanza de que los proyectos legítimos las utilicen. También secuestran cuentas npm de desarrolladores conocidos y luego plantan código malicioso dentro de bibliotecas populares.

El objetivo final es lanzar ataques o instalar puertas traseras dentro de aplicaciones creadas con los paquetes npm boobytrapped, que luego pueden usar para robar datos de los usuarios de esas aplicaciones.

Existen muchos casos de este tipo. En julio de 2018, un hacker comprometió la biblioteca ESLint con código malicioso, que fue diseñado para robar las credenciales npm de otros desarrolladores.

En agosto de 2017, el equipo de npm eliminó 38 paquetes npm de JavaScript que fueron capturados robando variables de entorno de otros proyectos, en un intento por recopilar información confidencial del proyecto, como contraseñas o claves API.

Usuarios de criptomonedas también son objetivos

Aunque este tipo de ataques por lo general se dirigen a desarrolladores, los intentos más recientes de puerta trasera de paquetes npm se han dirigido a usuarios de criptomonedas. Esto se debe a que JavaScript, e inherentemente npm, se utilizan para construir y potenciar muchas de las aplicaciones actuales de billeteras de criptomonedas basadas en web, móviles y de escritorio.

Los hackers a menudo abren puertas a las bibliotecas npm o crean clones atrapados, para plantar su código dentro de las billeteras y luego robar los fondos de los usuarios.

En junio de este año, el equipo de npm encontró código malicioso dentro de un paquete npm diseñado para robar seed de billeteras de criptomonedas y otras frases de acceso de inicio de sesión específicas para aplicaciones de criptografía.

La biblioteca fue utilizada por una startup de criptomonedas que decidió piratearse a sí misma antes de que los piratas informáticos pudieran explotar el error.

Otro ataque parecido ocurrió en noviembre de 2018, cuando los hackers modificaron un paquete npm utilizado por las aplicaciones de billetera móvil y de escritorio de Copay para poder robar bitcoins.