En otro caso de sabotaje, el desarrollador detrás del popular paquete NPM *«node-ipc»*, envió una nueva versión para protestar por la invasión de Ucrania por parte de Rusia, lo que generó preocupaciones sobre la seguridad en el código abierto y la cadena de suministro de software.

Los cambios, que afectaron a las versiones 10.1.1 y 10.1.2 de la biblioteca, introdujeron un comportamiento no deseado por parte de su mantenedor RIAEvangelist, apuntando a usuarios con direcciones IP ubicadas en Rusia o Bielorrusia, y borrando el contenido de archivos arbitrarios y reemplazándolos con un emoji de corazón.

Node-ipc es un módulo de nodo destacado que se utiliza para la comunicación entre procesos locales y remotos con soporte para Linux, macOS y Windows. Tiene más de 1.1 millones de descargas a la semana.

> *«Se producirá un abuso muy claro y un incidente crítico de seguridad de la cadena de suministro para cualquier sistema en el que se invoque este paquete NPM, si coincide con una ubicación geográfica de Rusia o Bielorrusia»,* dijo el investigador Synk Tal.

Al problema se le asignó el identificador CVE-2022-23812, con una calificación CVSS de 9.8. Los cambios del código malicioso se publicaron el 7 de marzo (versión 10.1.1), con una segunda actualización 10 horas más tarde (versión 10.1.1).

Aunque la carga útil destructiva se eliminó de la biblioteca con la versión 10.1.3, se envió una actualización importante después de menos de cuatro horas (versión 11.0.0), que importó otra dependencia llamada «peacenotwar«, también lanzada por RIAEvangelist como forma de *«protesta no violenta contra la agresión de Rusia».*

> *«Cada vez que se llama a la funcionalidad del módulo node-ipc, imprime en STDOUT un mensaje extraído del módulo de paz, no de guerra, y también coloca un archivo en el directorio del escritorio del usuario con contenidos relacionados con la situación actual en tiempos de guerra de Rusia y Ucrania»,* explicó Tal.

A partir del 15 de marzo de 2022, la última versión de node-ipc, 11.1.0, supera la versión del paquete «*peacenotwar*» de 9.1.3 a 9.1.5 y agrupa la biblioteca NPM de «*colors*«, al mismo tiempo que elimina los mensajes de la consola STDOUT.

Cabe mencionar que «*colors*«, junto con otro paquete llamado «*faker*«, fueron saboteados intencionalmente a inicios de enero por su desarrollador Marak Squires al introducir bucles infinitos en el código fuente, rompiendo efectivamente otras aplicaciones que dependían de las bibliotecas.

Según Bleeping Computer, que informó por primera vez sobre la corrupción, los cambios fueron una represalia, y el desarrollador dijo que *«respetuosamente, ya no voy a apoyar a Fortune 500 (y otras empresas de menor tamaño) con mi trabajo gratuito».*

En todo caso, la idea de usar módulos populares como «protestware» para implementar cargas destructivas y poner en peligro la cadena de suministro corre el riesgo de socavar la confianza en el software de código abierto.

> *«Este incidente de seguridad involucra actos destructivos de corrupción de archivos en el disco por parte de un mantenedor y sus intentos de ocultar y reafirmar ese sabotaje deliberado en distintas formas. Si bien este es un ataque con motivaciones impulsadas por protestas, destaca un problema mayor que enfrenta la cadena de suministro de software: las dependencias transitivas en su código pueden tener un gran impacto en su seguridad»,* dijo Tal.