La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), advirtió el viernes pasado sobre el malware de minería criptográfica incrustado en UAParser.js, una popular biblioteca NPM de JavaScript con más de 6 millones de descargas semanales, días después de que el repositorio de NPM se moviera para deshacerse de tres paquetes maliciosos que se encontraron para imitar la misma biblioteca

El ataque a la cadena de suministro dirigido a la biblioteca de código abierto vio tres versiones distintas, 0.7.29, 0.8.0, 1.0.0, que se publicaron con código malicioso el jueves luego de una toma de control exitosa de la cuenta NPM del mantenedor.

> *«Creo que alguien estaba secuestrando mi cuenta NPM y publicando algunos paquetes comprometidos (0.7.29, 0.8.0, 1.0.0) que probablemente instalan malware»,* dijo el desarrollador de UAParser.js, Faisal Salman.

El problema ya fue corregido con el lanzamiento de las versiones 0.7.30, 0.8.1 y 1.0.1.

Este desarrollo se produce días después de que la compañía de DevSecOps, Sonatype, revelara los detalles de tres paquetes, okhsa, klow y klown, que se hicieron pasar por la utilidad del analizador de cadenas de agente de usuario con el objetivo de extraer criptomonedas en sistemas Windows, macOS y Linux. No está claro hasta ahora si el mismo actor de la amenaza está detrás del último compromiso.

> *«Cualquier computadora que tenga este paquete instalado o en ejecución debe considerarse totalmente comprometida. Todos los secretos y claves almacenados en esa computadora deben rotarse de forma inmediata desde una computadora diferente. El paquete debe eliminarse, pero como el control total de la computadora puede haber sido otorgado a una entidad externa, no hay garantía de que al eliminar el paquete se elimine todo el software malicioso resultante de su instalación»,* dijo GitHub en una alerta independiente.