Se han detectado una serie de fallos de corrupción de memoria en la biblioteca de programación ncurses (abreviatura de nuevas maldiciones) que podrían ser aprovechados por actores maliciosos para ejecutar código maligno en sistemas vulnerables de Linux y macOS.

Los investigadores de Microsoft Threat Intelligence, Jonathan Bar Or, Emanuele Cozzi y Michael Pearse, han explicado en un informe técnico publicado hoy que, *«mediante la manipulación de variables de entorno, los atacantes podrían concatenar estas vulnerabilidades para aumentar sus privilegios y ejecutar código en el contexto del programa objetivo, o llevar a cabo otras acciones perniciosas».*

Estas vulnerabilidades, agrupadas bajo el nombre CVE-2023-29491 (con una puntuación CVSS de 7.8), han sido solucionadas desde abril de 2023. Microsoft también ha colaborado con Apple para abordar los problemas específicos de macOS relacionados con estas deficiencias.

Las variables de entorno son valores definidos por el usuario que pueden ser utilizados por múltiples programas en un sistema, y que pueden influir en el comportamiento de estos programas en el sistema. La manipulación de estas variables puede provocar que las aplicaciones realicen operaciones no autorizadas.

La auditoría de código y las pruebas de fuzzing de Microsoft revelaron que la biblioteca ncurses busca varias variables de entorno, incluyendo TERMINFO, que podrían ser contaminadas y combinadas con las deficiencias identificadas para lograr una escalada de privilegios. TERMINFO es una base de datos que permite a los programas utilizar terminales de visualización de manera independiente del dispositivo.

Las deficiencias abarcan una fuga de información de pila, una confusión de tipos de cadena parametrizada, un error de desbordamiento por uno, un desbordamiento de montón durante el análisis del archivo de base de datos TERMINFO y una denegación de servicio con cadenas canceladas.

> *«Las vulnerabilidades descubiertas podrían haber sido explotadas por atacantes para aumentar sus privilegios y ejecutar código dentro del contexto de un programa objetivo. No obstante, tomar el control de un programa mediante la explotación de deficiencias de corrupción de memoria requiere un ataque de varias etapas»,* señalaron los investigadores.

> *«Es posible que las deficiencias hubieran necesitado ser concatenadas entre sí para que un atacante aumentara sus privilegios, como explotar la fuga de información de la pila para obtener permisos de lectura arbitrarios junto con explotar el desbordamiento de montón para obtener un permiso de escritura».*