Una vulnerabilidad crítica recientemente identificada en el repositorio oficial de Homebrew Cask pudo haber permitido que piratas informáticos ejecuten código arbitrario en la máquinas de los usuarios con homebrew instalado.

La vulnerabilidad, que fue informada a los mantenedores el 18 de abril por un investigador de seguridad japonés llamado Ryotak, surgió de la forma en que se manejaron los cambios de código en su repositorio de GitHub, lo que resultó en un escenario en el que una solicitud de extracción maliciosa, es decir, los cambios propuestos, podría ser revisado y aprobado de forma automática. La falla fue solucionada el 19 de abril.

Homebrew es una solución de administración de paquetes de software de código abierto y gratuita, que permite la instalación de software en el sistema operativo macOS de Apple, así como en Linux. Homebrew Cask amplía la funcionalidad para incluir flujos de trabajo de línea de comandos para aplicaciones macOS basadas en GUI, fuentes, complementos y otro software de código no abierto.

> *«La vulnerabilidad descubierta permitiría a un atacante inyectar código arbitrario en un tonel y tiene que ser fusionado de forma automática. Esto se debe a una falla en la dependencia git_diff de la acción de GitHub review-cask-pr, que se utiliza para analizar la diferencia de una solicitud de extracción para su inspección. Debido a esta falla, el analizador puede falsificarse para ignorar por completo las líneas ofensivas, resultando en la aprobación exitosa de una solicitud de extracción maliciosa»*, dijo Markus Reiter, de Homebrew.

Esto significa que el código malicioso inyectado en el repositorio de Cask se fusionó sin ninguna revisión ni aprobación.

El investigador también envió una solicitud de extracción de prueba de concepto (PoC) que demuestra la vulnerabilidad, después de esto se revirtió. Con los hallazgos, Homebrew también eliminó la acción de GitHub *«automerge»*, así como deshabilitar y eliminar la acción de GitHub *«review-cask-pr»* de todos los repositorios vulnerables.

Además, se eliminó la capacidad de los bots de comprometerse con los repositorios *homebrew/cask**, y todas las solicitudes de extracción requieren una revisión manual y la aprobación de un mantenedor en el futuro. No se requiere ninguna acción por parte del usuario.

> *«Si esta vulnerabilidad fue abusada por un actor malicioso, podría ser utilizado para comprometer las máquinas que ejecutan brew antes de que se revirtió. Por eso creo firmemente que se requiere una auditoría de seguridad contra el ecosistema centralizado»*, dijo el investigador.