Se han descubierto dos graves fallos de seguridad críticos en el software de nube personal de código abierto conocido como CasaOS, los cuales podrían ser aprovechados con éxito por posibles atacantes para lograr la ejecución de código arbitrario y tomar el control de sistemas vulnerables.

Estas vulnerabilidades, identificadas como CVE-2023-37265 y CVE-2023-37266, ambas poseen una calificación CVSS de 9.8 sobre un máximo de 10.

El investigador de seguridad de Sonar, Thomas Chauchefoin, quien encontró estos problemas, explicó que *«permiten a los atacantes eludir los requisitos de autenticación y obtener acceso total al panel de control de CasaOS».*

Aún más preocupante, la capacidad de CasaOS para soportar aplicaciones de terceros podría ser empleada para ejecutar comandos arbitrarios en el sistema y lograr un acceso persistente al dispositivo o ingresar a las redes internas.

Luego de una divulgación responsable realizada el 3 de julio de 2023, los problemas de seguridad fueron abordados en la versión 0.4.4 lanzada por los mantenedores de IceWhale el 14 de julio de 2023.

Una breve descripción de estas dos fallas es la siguiente:

- CVE-2023-37265: Identificación errónea de la dirección IP de origen, lo cual posibilita que atacantes no autenticados ejecuten comandos arbitrarios con privilegios de administrador en instancias de CasaOS.
- CVE-2023-37266: Atacantes no autenticados pueden crear Tokens Web JSON (JWT) arbitrarios y acceder a funciones que requieren autenticación, además de ejecutar comandos arbitrarios con privilegios de administrador en instancias de CasaOS.

Si estas fallas se explotan con éxito, los atacantes podrían evadir las restricciones de autenticación y obtener privilegios administrativos en sistemas vulnerables de CasaOS.

> *«En términos generales, la identificación de direcciones IP en la capa de aplicación es propensa a riesgos y no debería ser utilizada como base para tomar decisiones de seguridad»,* indicó Chauchefoin.

> *«Existen diversos encabezados que pueden transportar esta información (como X-Forwarded-For o Forwarded, entre otros), y las API de lenguaje a veces necesitan interpretar matices del protocolo HTTP de manera uniforme. Del mismo modo, todos los marcos de trabajo tienen particularidades propias y pueden ser complicados de navegar sin un conocimiento experto de estos problemas comunes de seguridad».*