Los investigadores de seguridad cibernética revelaron dos vulnerabilidades de seguridad sin parchear, en el cargador de arranque U-Boot de código abierto.

Los problemas, que se descubrieron en el algoritmo de desfragmentación de IP implementado en U-Boot por NCC Group, podrían abusarse para lograr escritura arbitraria fuera de los límites y denegación de servicio (DoS).

U-Boot es un cargador de arranque que se utiliza en sistemas integrados basados en Linux, como ChromeOS, así como en lectores de libros electrónicos, como Amazon Kindle y Kobo eReader.

Las vulnerabilidades son las siguientes:

- CVE-2022-30790 (puntuación CVSS: 9.6): La sobrescritura del descriptor de agujeros en la desfragmentación de paquetes IP de U-Boot conduce a una primitiva de escritura arbitraria fuera de los límites.
- CVE-2022-30552 (puntuación CVSS: 7.1): Un gran desbordamiento de búfer conduce a DoS en el código de desfragmentación de paquetes IP de U-Boot.

Cabe mencionar que ambas fallas solo se pueden explotar desde la red local. Pero hacerlo puede permitir que un atacante rootee los dispositivos y provoquen un DoS al crear un paquete con formato incorrecto.

Se espera que los mantenedores de U-Boot resuelvan las deficiencias en un próximo parche, luego de lo cual se recomienda a los usuarios que actualicen a la última versión.