Un hacker de iOS y un investigador de seguridad cibernética publicaron ayer lo que se denominó como *«exploit de bootrom permanente no reparable»*, lo que significa, un jailbreak épico que funciona en todos los dispositivos iOS que van desde iPhone 4S (chip A5) hasta iPhone 8 y iPhone X (chip A11).

Apodado como Checkm8, el exploit aprovecha las debilidades de seguridad incompatibles en Bootrom (SecureROM) de Apple, el primer código significativo que se ejecuta en un iPhone durante el arranque, que de ser explotado, proporciona un mayor nivel de acceso al sistema.

> *«EPIC JAILBREAK: Presentamos checkm8, un exploit de bootrom permanente e incompatible para cientos de millones de dispositivos iOS»*, dijo axi0mX al anunciar el lanzamiento en Twitter.

El nuevo exploit se produjo exactamente un mes después de que Apple lanzara un parche de emergencia para otra vulnerabilidad crítica de jailbreak que funciona en dispositivos Apple, incluyendo el iPhone XS, XS Max y XR, además del iPad Mini, iPad Air 2019, con iOS 12.4 e iOS 12.2 o anterior.

Ya que los exploits de bootrom son problemas a nivel de hardware y no se pueden reparar sin una revisión de hardware, una simple actualización de software no puede abordar el problema.

Cabe mencionar que el exploit checkm8 en sí mismo no es un jailbreak completo con Cydia, sino un exploit que los investigadores y la comunidad de kailbreak pueden utilizar para desarrollar una herramienta de jailbreak completamente funcional.

Las características que el exploit checkm8 permite incluyen las siguientes:

- Jailbreak y degradación de iPhone 3GS (nuevo bootrom) con exploc bootc alote8 sin ataduras
- Modo DFU Pwned con steaks4uce exploit para dispositivos S5L8720

- Modo DFU Pwned con exploit limera1n para dispositivos S5L8920/S5L8922
- Modo DFU Pwned con exploit SHAtter para dispositivos S5L8930
- Volcar SecureROM en dispositivos S5L8920/S5L8922/S5L8930
- Volcado NOR en dispositivos S5L8920
- Flash NOR en dispositivos S5L8920
- Cifrar o descifrar datos hexadecimales en un dispositivo conectado en modo DFU pwned utilizando la clave GID o UID

> *«Esta es posiblemente la noticia más importante en la comunidad de jailbreak de iOS en años. Estoy lanzando mi exploit de forma gratuita para beneficio de la comunidad de investigación de jailbreak y seguridad de iOS»,* dijo axi0mX, quien lanzó el exploit en GitHub.
>
> *«Los investigadores y desarrolladores pueden usarlo para volcar SecureROM, descifrar los keybags con el motor AES y degradar el dispositivo para habilitar JTAG. Todavía necesita hardware y software adicional para usar JTAG»,* agregó.

Axi0mX dice que descubrió la vulnerabilidad de bootrom subyacente mientras analizaba un parche de seguridad que Apple lanzó en 2018 para abordar una vulnerabilidad crítica de uso posterior libre descubierta anteriormente en el código USB de iBoot.

Además, dice que su exploit no se puede realizar de forma remota. Solo se puede activar por medio de USB y requiere acceso físico.

El jailbreak solo funciona en iPhones que ejecutan los conjuntos de chips A5 y A11 de Apple y no funciona ne los dos últimos conjuntos de chips, es decir, A12 y A13.