Se descubrió una serie de vulnerabilidades críticas en los conjuntos de chips de Qualcomm que podrían permitir a los hackers comprometer dispositivos Android de forma remota al enviar paquetes maliciosos por el aire sin interacción del usuario.

Descubiertas por investigadores de seguridad de Tencent Blade, las vulnerabilidades, conocidas como QualPwn, residen en el firmware de WLAN y módem de los conjuntos de chips Qualcomm que alimentan cientos de millones de teléfonos inteligentes y tabletas con Android.

Según los investigadores, existen principalmente dos vulnerabilidades críticas en los conjuntos de chips de Qualcomm y una en el controlador de kernel de Linux de Qualcomm para Android, que de encadenarse juntos, podrían permitir a los atacantes tomar el control completo de los dispositivos Android específicos dentro de su rango de WiFi.

> *«Una de las vulnerabilidades permite a los atacantes comprometer la WLAN y el módem por aire. La otra permite a los atacantes comprometer el kernel de Android desde el chip WLAN. La cadena de explotación completa permite a los atacantes comprometer el kernel de Android en algunas circunstancias»,* dijeron los investigadores.

Las vulnerabilidades son:

- CVE-2019-10539 (WLAN comprometida): La primera falla es un problema de desbordamiento de búfer que reside en el firmaware de Qualcomm WLAN debido a la falta de verificación de longitud al analizar la longitud del encabezado IE de límite extendido.
- CVE-2019-10540 (Problema de WLAN en módem): El segundo problema también es una falla de desbordamiento de búfer que reside en el firmware de Qualcomm WLAN y afecta su función de red de área vecina (NAN) debido a la falta de verificación del valor de recuento recibido en el atributo de disponibilidad NAN.
- CVE-2019-10538 (Problema del módem en el kernel de Linux): El tercer problema

radica en el controlador del kernel de Linux de Qualcomm para Android que puede explotarse enviando posteriormente entradas maliciosas desde el conjunto de chips de WiFi para sobrescribir partes del kernel de Linux que ejecuta el Android principal del dispositivo.

Una vez comprometido, el núcleo brinda a los atacantes acceso completo al sistema, incluida la capacidad de instalar rootkits, extraer información confidencial y realizar otras acciones maliciosas, todo mientras evade la detección.

Aunque los investigadores de Tencent probaron sus ataques QualPwn contra los dispositivos Google Pixel 2 y Pixel 3 que se ejecutan en chips Qualcomm Snapdragon 835 y Snapdragon 845, las vulnerabilidades afectan a muchos otros conjuntos de chips, según un aviso publicado por Qualcomm.

> *«IPQ8074, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574, QCA6574AU, QCA6584, QCA8081, QCA9379, QCS404, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, SXR1130»*

Los investigadores descubrieron las vulnerabilidades de QualPwn en febrero y marzo de este año y las informaron de forma responsable a Qualcomm, quien luego lanzó parches en junio y notificó a los OEM, incluidos Google y Samsung.

Google lanzó ayer parches de seguridad para estas vulnerabilidades como parte de su Boletín de seguridad de Android de agosto de 2019. Por lo tanto, se recomienda descargar los parches de seguridad tan pronto como estén disponibles.

Ya que los teléfonos Android son muy lentos para recibir actualizaciones de parches, los investigadores decidieron no revelar detalles técnicos completos o cualquier vulnerabilidad

de PoC para estas vulnerabilidades en el corto plazo, dando a los usuarios finales suficiente tiempo para recibir actualizaciones de los fabricantes de sus dispositivos.