INVESTIGADORES ALERTAN DE FALLO EN EQUIPOS WIFI REALTEK (04/JUNIO/2021)
Investigadores alertan de fallo en equipos Wifi Realtek (04/junio/2021)

Varias vulnerabilidades en el módulo Wifi de ciertos equipos Realtek podrían permitir que un atacante obtenga escalamiento de privilegios y capturas las comunicaciones inalámbricas que pasen a través de estos equipos vulnerables.

En la actualidad una de las características más utilizadas en los dispositivos que pertenecen a las tecnologías de la información y comunicación TICs, es la conexión inalámbrica, específicamente mediante la tecnología Wifi que permite la conexión móvil a redes tanto privadas como públicas que ofrecen acceso inalámbrico. La gran mayoría de fabricantes de dispositivos TICs incluyen elementos de hardware y software que aseguren a sus usuarios una fácil y eficiente conexión a redes inalámbricas.

Un fallo en el módulo Wifi RTL8170C permitiría el control total de manera remota del módulo de las conexiones inalámbricas y el escalamiento de privilegios de tipo root en los sistemas operativos de tipo Android y Linux. Fallas similares encontradas anteriormente en varios módulos wiki de Realtek ya han sido priorizadas de acuerdo a los reportes CVE-2020-9395, CVE-2020-27301 y CVE-2020-27302.

En consideración al alto riesgo contra la confidencialidad de los sistemas de información en los cuales se encuentren instalados los módulos Wifi de Realtek vulnerables, el EcuCERT recomienda a su comunidad objetivo, tomar en consideración las siguientes recomendaciones:

1. Actualizar el software de los equipos Realtek, utilizando los enlaces de descarga establecidos por el fabricante.
2. Ejecutar aplicaciones con perfiles de usuarios con el menor privilegio posible.
3. Instalar y actualizar aplicaciones antivirus.

Referencias

SecurityWeek (2021). Vulnerabilities in Realtek Wi-Fi Module Expose Many Devices to Remote Attacks. Disponible en https://www.securityweek.com/vulnerabilities-realtek-wi-fi-module-expose-many-devices-remote-attacks

CVE (2020). CVE-2020-9395 Disponible en https://nvd.nist.gov/vuln/detail/CVE-2020-9395

CVE (2020). CVE-2020-27301 Disponible en https://nvd.nist.gov/vuln/detail/CVE-2020-27301

CVE (2020). CVE-2020-27302 Disponible en https://nvd.nist.gov/vuln/detail/CVE-2020-27302