Investigadores de seguridad cibernética advierten sobre un aumento en los intentos de explotación que usan como arma una vulnerabilidad crítica de ejecución remota de código en Realtek Jungle SDK desde inicios de agosto de 2022.

Según Unit42 de Palo Alto Networks, se cree que la campaña en curso registró 134 millones de intentos de explotación hasta diciembre de 2022, con el 97% de los ataques ocurridos en los últimos cuatro meses.

Cerca del 50% de los ataques se originaron en Estados Unidos (48.3%), seguido de Vietnam (17.8%), Rusia (14.6%), Países Bajos (7.4%), Francia (6.4%), Alemania (2.3%) y Luxemburgo (1.6%).

Además, el 95% de los ataques que aprovecharon la deficiencia de seguridad que emanaba de Rusia apuntaron a organizaciones en Australia.

> *«Muchos de los ataques que observamos intentaron entregar malware para infectar dispositivos IoT vulnerables. Los grupos de amenazas están utilizando esta vulnerabilidad para llevar a cabo ataques a gran escala en dispositivos inteligentes en todo el mundo»,* dijeron los investigadores de Unit42.

La vulnerabilidad en cuestión es CVE-2021-35394 (puntaje CVSS: 9.8), un conjunto de desbordamientos de búfer y un error de inyección de comando arbitrario que podría armarse para ejecutar código arbitrario con el nivel más alto de privilegios y hacerse cargo de los dispositivos afectados.

ONEKEY (antes IoT Inspector), reveló los problemas en agosto de 2021. La vulnerabilidad afecta a una amplia gama de dispositivos de D-Link, LG, Belkin, ASUS y NETGEAR.

Unit42 dijo que descubrió tres tipos diferentes de cargas útiles distribuidas como resultado de la explotación salvaje de la vulnerabilidad:

- Un script ejecuta un comando de shell en el servidor de destino para descargar malware adicional
- Un comando inyectado que escribe una carga útil binaria en un archivo y lo ejecuta
- Un comando inyectado que reinicia directamente el servidor de destino para provoar una condición de denegación de servicio (DoS)

También se entregan a través del abuso de CVE-2021-35394 botnets conocidas como Mirai, Gafgyt y Mozi, así como una nueva botnet de denegación de servicio distribuido (DoS) basada en Golang denominada RedGoBot.

Observada por primera vez en septiembre de 2022, la campaña RedGoBot consiste en lanzar un script de shell que está diseñado para descargar una serie de clientes de botnet adaptados a distintas arquitecturas de CPU. El malware, una vez lanzado, está equipado para ejecutar comandos del sistema operativo y montar ataques DDoS.

Los hallazgos subrayan una vez más la importancia de actualizar el software de forma oportuna para evitar la exposición a amenazas potenciales.

> *«El aumento de los ataques que aprovechan CVE-2021-35394 muestra que los atacantes están muy interesados en las vulnerabilidades de la cadena de suministro, que pueden ser difíciles de identificar y corregir para el usuario promedio. Estos problemas pueden dificultar que el usuario afectado identifique los productos intermedios específicos que se están explotando»,* agregaron los investigadores.