Se han revelado múltiples vulnerabilidades de seguridad en el sistema operativo LG webOS, utilizado en sus televisores inteligentes, las cuales podrían ser aprovechadas para eludir la autorización y obtener acceso de root en los dispositivos.

Los descubrimientos provienen de la firma de ciberseguridad rumana Bitdefender, que detectó y reportó las fallas en noviembre de 2023. LG ha corregido los problemas como parte de las actualizaciones lanzadas el 22 de marzo de 2024.

Las vulnerabilidades están identificadas desde CVE-2023-6317 hasta CVE-2023-6320 y afectan a las siguientes versiones de webOS:

- webOS 4.9.7 – 5.30.40 en LG43UM7000PLA
- webOS 5.5.0 – 04.50.51 en OLED55CXPUA
- webOS 6.3.3-442 (kisscurl-kinglake) – 03.36.50 en OLED48C1PUB
- webOS 7.3.1-43 (mullet-mebin) – 03.33.85 en OLED55A23LA

Una breve descripción de las deficiencias es la siguiente:

- CVE-2023-6317: Una vulnerabilidad que permite a un atacante evitar la verificación de PIN y agregar un perfil de usuario privilegiado al televisor sin necesidad de interacción del usuario.
- CVE-2023-6318: Una vulnerabilidad que permite al atacante elevar sus privilegios y obtener acceso de root para tomar el control del dispositivo.
- CVE-2023-6319: Una vulnerabilidad que permite la inyección de comandos del sistema operativo al manipular una biblioteca llamada asm, encargada de mostrar letras de canciones.
- CVE-2023-6320: Una vulnerabilidad que permite la inyección de comandos autenticados al manipular el punto final de API com.webos.service.connectionmanager/tv/setVlanStaticAddress.

La explotación exitosa de las fallas podría permitir a un actor malintencionado obtener permisos elevados en el dispositivo, los cuales podrían combinarse con CVE-2023-6318 y

CVE-2023-6319 para obtener acceso de root, o con CVE-2023-6320 para ejecutar comandos arbitrarios como usuario dbus.

> *«Aunque el servicio vulnerable está destinado solo para acceso LAN, Shodan, el motor de búsqueda de dispositivos conectados a Internet, identificó más de 91,000 dispositivos que exponen este servicio a la Internet»,* señaló Bitdefender. La mayoría de los dispositivos se encuentran en Corea del Sur, Hong Kong, EE. UU., Suecia, Finlandia y Letonia.