Actores maliciosos están explotando activamente fallos de seguridad en dispositivos IoT de GeoVision que han llegado al final de su vida útil (EoL), con el fin de integrarlos en una botnet Mirai utilizada para lanzar ataques de denegación de servicio distribuido (DDoS).

Esta actividad fue detectada por primera vez a inicios de abril de 2025 por el equipo de Inteligencia y Respuesta de Seguridad de Akamai (SIRT). Los atacantes están aprovechando dos vulnerabilidades de inyección de comandos en el sistema operativo (CVE-2024-6047 y CVE-2024-11120, ambas con una puntuación CVSS de 9.8) que permiten la ejecución de comandos arbitrarios.

> *"El ataque se enfoca en el endpoint `/DateSetting.cgi` de los dispositivos IoT de GeoVision e inyecta comandos maliciosos en el parámetro `szSrvIpAddr`,"* explicó el investigador de Akamai, Kyle Lefton, en un informe.

En los ataques observados por la empresa de seguridad web e infraestructura, se detectó que la botnet descarga y ejecuta una versión para arquitectura ARM del malware Mirai llamada LZRD.

Además de las fallas en los dispositivos de GeoVision, la botnet también explota otras vulnerabilidades conocidas, como una del sistema Hadoop YARN (CVE-2018-10561) y otra reportada en diciembre de 2024 que afecta a dispositivos DigiEver.

Existen indicios que sugieren que esta campaña está relacionada con actividades previas conocidas bajo el nombre InfectedSlurs.

> *"Una de las formas más efectivas para que los ciberdelincuentes formen una botnet es atacar dispositivos con firmware antiguo y mal protegido. Muchos fabricantes no proporcionan actualizaciones para equipos retirados del mercado, y en algunos casos, la empresa ya ni siquiera existe»,* advirtió Lefton.

Dado que es poco probable que los dispositivos afectados de GeoVision reciban parches de seguridad, se recomienda a los usuarios reemplazarlos por modelos más recientes para reducir el riesgo.

Vulnerabilidad en Samsung MagicINFO también está siendo usada para propagar Mirai

Esta advertencia coincide con reportes de Arctic Wolf y el Instituto de Tecnología SANS, que informan sobre la explotación activa de la vulnerabilidad CVE-2024-7399 (con un puntaje CVSS de 8.8), una falla de recorrido de directorios en el servidor Samsung MagicINFO 9. Esta brecha permite que un atacante escriba archivos arbitrarios con privilegios de sistema, lo que facilita la instalación del malware Mirai.

Aunque Samsung solucionó este problema en agosto de 2024, los atacantes comenzaron a utilizarlo tras la publicación de un código de prueba (PoC) el 30 de abril de 2025. El exploit permite recuperar y ejecutar un script que descarga la botnet.

> *"La vulnerabilidad permite a usuarios no autenticados escribir archivos de manera arbitraria, lo que puede derivar en ejecución remota de código si se insertan archivos JSP diseñados específicamente,"* indicó Arctic Wolf.

Se recomienda actualizar los sistemas a la versión 21.1050 o superior para reducir el riesgo de explotación.