Investigadores de ciberseguridad han identificado tres vulnerabilidades en los switches industriales WGS-804HPT de Planet Technology. Estas fallas pueden combinarse para permitir la ejecución remota de código sin necesidad de autenticación previa en dispositivos afectados.

> *«Estos dispositivos son ampliamente empleados en sistemas de automatización de hogares y edificios para diversas aplicaciones de red. Un atacante que logre controlar remotamente uno de estos switches puede utilizarlos como punto de acceso para comprometer otros dispositivos en la red interna y avanzar lateralmente»,* explicó Tomer Goldschmidt de Claroty en un informe publicado el jueves.

La empresa de seguridad en tecnología operativa llevó a cabo un análisis detallado del firmware de estos switches utilizando la herramienta QEMU. Determinaron que las vulnerabilidades se encuentran en la interfaz `dispatcher.cgi`, que proporciona servicios web. A continuación, se detallan las fallas detectadas:

- CVE-2024-52558 (puntuación CVSS: 5.3): Un error de subdesbordamiento de entero que permite a un atacante no autenticado enviar una solicitud HTTP malformada, lo que puede causar el bloqueo del dispositivo.
- CVE-2024-52320 (puntuación CVSS: 9.8): Una vulnerabilidad de inyección de comandos en el sistema operativo que permite a un atacante no autenticado ejecutar comandos mediante una solicitud HTTP maliciosa, lo que facilita la ejecución remota de código.
- CVE-2024-48871 (puntuación CVSS: 9.8): Un desbordamiento de búfer basado en la pila que puede ser explotado a través de una solicitud HTTP maliciosa, permitiendo la ejecución remota de código.

Si estas vulnerabilidades son explotadas con éxito, un atacante podría alterar el flujo de ejecución del dispositivo al insertar un shellcode en la solicitud HTTP, obteniendo así acceso para ejecutar comandos en el sistema operativo.

Tras recibir el reporte de manera responsable, la compañía taiwanesa publicó correcciones para abordar estas fallas en la versión 1.305b241111, lanzada el 15 de noviembre de 2024.