Una vulnerabilidad de seguridad sin parchear en la cámara de red Edimax IC-7100 está siendo explotada por ciberdelincuentes para distribuir variantes del malware de la botnet Mirai desde al menos mayo de 2024.

La falla, identificada como CVE-2025-1316 (con una puntuación de 9.3 en CVSS v4), es una vulnerabilidad crítica de inyección de comandos en el sistema operativo. Los atacantes pueden aprovecharla para ejecutar código de manera remota en dispositivos vulnerables mediante solicitudes especialmente diseñadas.

Según la empresa de seguridad Akamai, los primeros intentos de explotación de esta vulnerabilidad datan de mayo de 2024, aunque un exploit de prueba de concepto (PoC) ha estado disponible públicamente desde junio de 2023.

Investigadores de Akamai, Kyle Lefton y Larry Cashdollar, explicaron que el exploit ataca el endpoint `/camera-cgi/admin/param.cgi` en los dispositivos Edimax e inyecta comandos en la opción `NTP_serverName`, dentro del parámetro `ipcamSource` de `param.cgi`.

Aunque el ataque requiere autenticación, los atacantes han estado utilizando credenciales predeterminadas (admin:1234) para obtener acceso no autorizado.

Se han identificado al menos dos variantes de la botnet Mirai que explotan esta vulnerabilidad. Una de ellas, además, incorpora mecanismos anti-depuración antes de ejecutar un script que descarga el malware en distintas arquitecturas.

El propósito final de estos ataques es reclutar dispositivos comprometidos en una red capaz de llevar a cabo ataques distribuidos de denegación de servicio (DDoS) contra objetivos específicos mediante los protocolos TCP y UDP.

Además, se ha detectado que estas botnets también están explotando otras vulnerabilidades, como CVE-2024-7214 (que afecta a dispositivos IoT de TOTOLINK), CVE-2021-36220 y una falla en Hadoop YARN.

Por su parte, Edimax publicó un aviso independiente la semana pasada, en el que confirmó que CVE-2025-1316 afecta a dispositivos antiguos que ya no reciben soporte y que no se lanzará un parche de seguridad, ya que el modelo en cuestión fue descontinuado hace más de 10 años.

Ante la falta de una solución oficial, se recomienda a los usuarios actualizar a un modelo más reciente o, en su defecto, evitar exponer el dispositivo directamente en internet, cambiar la contraseña predeterminada del administrador y monitorear los registros de acceso en busca de actividad sospechosa.

Akamai advierte que una de las formas más comunes en que los ciberdelincuentes construyen botnets es explotando dispositivos con firmware obsoleto y mal protegido.

«El legado de Mirai sigue afectando a organizaciones en todo el mundo, y la proliferación de botnets basadas en este malware no muestra signos de detenerse. Con numerosos tutoriales y código fuente disponible de forma gratuita (y ahora con la ayuda de la IA), crear una botnet es más fácil que nunca.»