Una variante de la botnet Mirai conocida como MooBot está integrando dispositivos D-Link vulnerables en un ejército de bots de denegación de servicio aprovechando múltiples vulnerabilidades.

> *«Si los dispositivos se ven comprometidos, los atacantes los controlarán completamente, y podrían utilizar esos dispositivos para realizar más ataques, como ataques distribuidos de denegación de servicio (DDoS)»*, dijo Unit42 de Palo Alto Networks.

MooBot, revelado por primera vez por el equipo Netlab de Qihoo 360 en septiembre de 2019, se centró previamente en las grabadoras de video digital LILIN y los productos de videovigilancia de Hikvision para expandir su red.

En la última ola de ataques descubierta por Unit42 a inicios de agosto de 2022, hasta cuatro vulnerabilidades distintas en los dispositivos D-Link, tanto antiguos como nuevos, allanaron el camino para la implementación de muestras de MooBot. Estas incluyen:

- CVE-2015-2051 (puntuación CVSS: 10): Vulnerabilidad de ejecución de comando de encabezado de acción HNAP SOAPA de D-Link
- CVE-2018-6530 (puntuación CVSS: 9.8): Vulnerabilidad de ejecución remota de código de la interfaz SOAP de D-Link
- CVE-2022-26258 (puntuación CVSS: 9.8): Vulnerabilidad de ejecución de comandos remotos de D-Link
- CVE-2022-28958 (puntuación CVSS: 9.8): Vulnerabilidad de ejecución de comandos remotos de D-Link

La explotación exitosa de las vulnerabilidades mencionadas podría conducir a la ejecución remota de código y la recuperación de una carga útil de MooBot desde un host remoto, que

después analizar las instrucciones de un servidor de comando y control (C2) para lanzar un ataque DDoS en una dirección IP específica y número de puerto.

Se recomienda a los usuarios de estos dispositivos que apliquen parches y actualizaciones publicados por la compañía para mitigar las posibles amenazas.

> *«Las vulnerabilidades tienen una complejidad de ataque baja pero un impacto de seguridad crítico que puede conducir a la ejecución remota de código. Una vez que el atacante obtiene el control de esta forma, podría aprovechar al incluir los dispositivos recientemente comprometidos en su botnet para realizar más ataques como DDoS»,* dijeron los investigadores.