USTIC-AV 10/22. Explotación de vulnerabilidades críticas en routers D-Link (09/09/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones avisa de la publicación esta semana de una serie de ataques con intentos de **explotación de hasta cuatro vulnerabilidades críticas diferentes** e n **dispositivos D-Link**.

Detalle

Se ha descubierto que la ***botnet* MooBot está aprovechando vulnerabilidades no parcheadas en routers D-Link para incrementar los dispositivos controlados.**

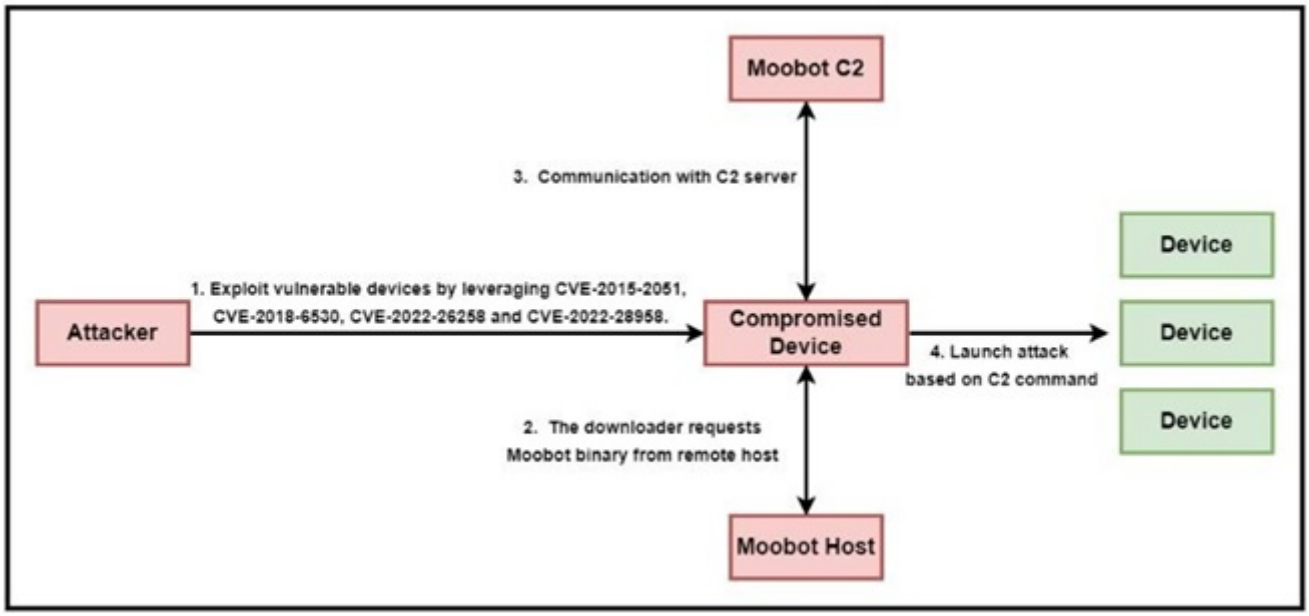
MooBot, revelado por primera vez por el equipo Netlab de Qihoo 360 en septiembre de 2019, se centró previamente en las grabadoras de video digital LILIN y los productos de videovigilancia de Hikvision para expandir su red. Hoy el *malware* ha actualizado su alcance de orientación, que es típico de las *botnets* que buscan grupos sin explotar de dispositivos vulnerables que puedan atrapar.

A principios del pasado mes de agosto, la Unidad 42 de Palo Alto Networks observó una serie de ataques con intentos de **ex plotación de hasta cuatro vulnerabilidades** en dispositivos D-Link, tanto antiguos como nuevos:

- CVE-2015-2051 (puntuación CVSS: 10,0): vulnerabilidad de ejecución de comando a través de la acción *'GetDevice Settings'* en la interfaz HNAP.
- CVE-2018-6530 (puntuación CVSS: 9,8): vulnerabilidad de inyección remota de comandos del sistema operativo a través de un parámetro en la interfaz SOAP.
- CVE-2022-26258 (puntuación CVSS: 9,8): vulnerabilidad de ejecución de comandos remotos a través de un parámetro en*'lan.asp'*.
- CVE-2022-28958 (puntuación CVSS: 9,8): vulnerabilidad de ejecución remota de código a través de un parámetro en *'shareport.php'*.

El proveedor ha lanzado actualizaciones de seguridad para abordar estas vulnerabilidades, pero no todos los usuarios han aplicado los parches todavía, especialmente los dos últimos, que se dieron a conocer en marzo y mayo de este año.

La explotación exitosa de alguna de **las vulnerabilidades** anteriores **podría conducir a la ejecución remota de comandos o código** y permitir la recuperación de la carga útil de MooBot desde un servidor remoto. A partir de aquí, el dispositivo permanecería a la espera de instrucciones del servidor de comando y control (C2) para ejecutar, por ejemplo, **ata ques distribuidos de denegación de servicio (DDoS)**.



Esquema de la campaña. Fuente: unit42.paloaltonetworks.com

Los usuarios de dispositivos D-Link comprometidos pueden notar caídas en la velocidad de Internet, falta de respuesta, sobrecalentamiento del enrutador o cambios inexplicables en la configuración de DNS, todos signos comunes de infecciones de *botnet*.

Debido a la criticidad, rogamos encarecidamente que se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas para hacer frente a las vulnerabilidades.

Sistemas Afectados

- **Dispositivos D-Link:**
  - DIR-65L
  - DIR-645
  - DIR816L
  - DIR-820L
  - DIR-860L
  - DIR-868L
  - DIR-880L

Recomendaciones Actualizadas (09/09/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas informáticos:

Mitigación

1º. Solución a las vulnerabilidades:

Aplicar las **actualizaciones de seguridad y parches disponibles en la página oficial del fabricante** para mitigar potenciales amenazas.

Referencias

- **Publicaciones sobre la explotación de las vulnerabilidades:**
  - https://unit42.paloaltonetworks.com/moobot-d-link-devices/
  - https://www.bleepingcomputer.com/news/security/moobot-botnet-is-coming-for-your-unpatched-d-link-router/
  - https://unaaldia.hispasec.com/2022/09/routers-d-link-en-el-punto-de-mira-de-moobot.html
  - https://thehackernews.com/2022/09/mirai-variant-moobot-botnet-exploiting.html
- **Ataques anteriores:**
  - https://unaaldia.hispasec.com/2022/08/mas-de-80-000-camaras-hikvision-expuestas-por-una-vulnerabilidad.html
  - https://unaaldia.hispasec.com/2020/03/multiples-botnets-utilizaron-0-days-en-dispositivos-de-grabacion-de-video-digital-lilin.html

---

En caso de haber detectado la explotación de estas vulnerabilidades :

debe reportar el incidente mediante correo electrónico a sau.cges.sspa@juntadeandalucia.es indicando en el *Asunto: [Compromiso Dlink0922]*

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud