Se observó que una variante de la botnet Mirai, llamada Beastmode, adopta vulnerabilidades recientemente reveladas en los enrutadores TOTOLINK entre febrero y marzo de 2022, con el fin de infectar dispositivos sin parches y expandir su alcance potencialmente.

> *«La campaña DDoS basada en Mirai Beastmode (también conocido como B3astmode), actualizó agresivamente su arsenal de exploits. Se agregaron cinco nuevos exploits en un mes, con tres dirigidos a varios modelos de routers TOTOLINK»,* dijo el equipo de investigación de FortiGuard Labs de Fortinet.

La lista de vulnerabilidades explotadas en los routers TOTOLINK es la siguiente:

- CVE-2022-26210 (puntaje CVSS: 9.8): Una vulnerabilidad de inyección de comandos que podría explotarse para obtener la ejecución de código arbitrario.
- CVE-2022-26186 (puntaje CVSS: 9.8): Una vulnerabilidad de inyección de comando que afecta a los routers TOTOLINK N600R y A7100 RU.
- CVE-2022-25075 a CVE-2022-25084 (puntajes CVSS: 9.8): Vulnerabilidades de inyección de comandos que afectan a varios routers TOTOLINK, lo que lleva a la ejecución de código.

Los otros exploits a los que apunta Beastmode, incluyen fallas en la cámara IP TP-LINK Tapo C200 (CVE-2021-4045, puntaje CVSS: 9.8), routers Huawei HG532 (CVE-2017-17215, puntaje CVSS: 8.8), soluciones de videovigilancia de NUUO y Netgear (CVE-2016-5674, puntuación CVSS: 9.8) y productos D-Link descontinuados (CVE-2021-45382, puntuación CVSS: 9.8).

Para evitar que los modelos afectados se apoderen de la red de bots, es recomendable que los usuarios actualicen sus dispositivos con el firmware más reciente.

> *«Aunque el autor original de Mirai fue arrestado en el otoño de 2018, destaca cómo los actores de amenazas, como los que están detrás de la campaña Beastmode, siguen incorporando rápidamente el código de explotación recientemente publicado*

> *para infectar dispositivos sin parches usando el malware Mirai»,* dijeron los investigadores.