La Agencia de Seguridad Cibernética y Protección de Infraestructura de Estados Unidos (CISA) ha añadido ocho vulnerabilidades a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), basándose en evidencia de explotación activa.

Esto incluye seis fallos que afectan a los teléfonos inteligentes de Samsung y dos vulnerabilidades que impactan a dispositivos de D-Link. Todas las debilidades han sido solucionadas a partir de 2021.

- CVE-2021-25394 (puntuación CVSS: 6.4) – Vulnerabilidad de condición de carrera en dispositivos móviles Samsung.
- CVE-2021-25395 (puntuación CVSS: 6.4) – Vulnerabilidad de condición de carrera en dispositivos móviles Samsung.
- CVE-2021-25371 (puntuación CVSS: 6.7) – Una vulnerabilidad no especificada en el controlador DSP utilizado en dispositivos móviles Samsung que permite la carga de bibliotecas ELF arbitrarias.
- CVE-2021-25372 (puntuación CVSS: 6.7) – Verificación de límites incorrecta en el controlador DSP de dispositivos móviles Samsung.
- CVE-2021-25487 (puntuación CVSS: 7.8) – Vulnerabilidad de lectura fuera de límites en dispositivos móviles Samsung que conduce a la ejecución arbitraria de código.
- CVE-2021-25489 (puntuación CVSS: 5.5) – Vulnerabilidad de validación incorrecta de entrada en dispositivos móviles Samsung que resulta en una interrupción del sistema.
- CVE-2019-17621 (puntuación CVSS: 9.8) – Una vulnerabilidad de ejecución remota de código sin autenticación en el enrutador D-Link DIR-859.
- CVE-2019-20500 (puntuación CVSS: 7.8) – Una vulnerabilidad de inyección de comandos de sistema operativo autenticada en D-Link DWL-2600AP.

La adición de las dos vulnerabilidades de D-Link se produce después de un informe de Palo Alto Networks Unit 42 el mes pasado sobre actores de amenazas asociados con una variante de botnet Mirai que aprovecha fallos en varios dispositivos IoT para propagar el malware en una serie de ataques que comenzaron en marzo de 2023.

Sin embargo, no está claro cómo se están aprovechando los fallos en los dispositivos

Samsung en la naturaleza. Pero dada la naturaleza del objetivo, es probable que hayan sido utilizados por un proveedor de software espía comercial en ataques altamente dirigidos.

Es importante destacar que Google Project Zero reveló un conjunto de fallos en noviembre de 2022 que, según afirmaron, fueron utilizados como parte de una cadena de exploits dirigidos a los teléfonos Samsung.

Ante la explotación activa, se requiere que las agencias del Poder Ejecutivo Civil Federal (FCEB) apliquen las correcciones necesarias antes del 20 de julio de 2023 para asegurar sus redes contra posibles amenazas.