Nro. Alerta:	AL-2025-039	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	07-ago-2025	Vulnerabilidades en Dispositivos D-Link (modelos DCS-2530L, DCS-2670L y DNR-322L)	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Explotación activa de vulnerabilidades
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Vulnerabilidades en Dispositivos D-Link (modelos DCS-2530L, DCS-2670L y DNR-322L) - figura referencial

Se han identificado múltiples vulnerabilidades en dispositivos D-Link (modelos DCS-2530L, DCS-2670L y DNR-322L), que están siendo explotadas actualmente. Estas fallas permiten a actores maliciosos acceder a contraseñas sin autenticación y ejecutar comandos remotos. La CISA ha incluido estas vulnerabilidades en su catálogo KEV (Known Exploited Vulnerabilities).

III. INTRODUCCIÓN

D-Link es un proveedor popular de cámaras de seguridad y video grabadora de red. Sus dispositivos, comúnmente usados en entornos domésticos y empresariales, presentan fallas graves que comprometen la confidencialidad y disponibilidad de las redes a las que están conectados. La CISA y otras organizaciones de ciberseguridad han emitido advertencias urgentes para mitigar los riesgos.

IV. VECTOR DE ATAQUE

El vector de ataque se basa en la explotación remota de vulnerabilidades antiguas, pero aún presentes en Dispositivos D-Link no actualizados o fuera de soporte. Las vulnerabilidades utilizadas son:

CVE-2020-25078 (CVSS 7.5 AV:N): Permite a un atacante no autenticado acceder remotamente a la contraseña del administrador mediante un endpoint expuesto en los modelos DCS-2530L y DCS-2670L.

CVE-2020-25079 (CVSS 8.8 AV:N): Con enumeración cwe-77 de inyección de comando. Permite a un atacante autenticado ejecutar comandos arbitrarios a través de inyección en el componente cgi-bin/ddns_enc.cgi, afectando los mismos modelos.

CVE-2022-40799 (CVSS 8.8 AV:N): Afecta al video grabadora de red DNR-322L, este permite a un atacante autenticado descargar y ejecutar código sin validación de integridad, obteniendo acceso a nivel de sistema operativo, catalogada como cwe-494.

A pesar de que estas vulnerabilidades fueron divulgadas entre 2020 y 2022, muchas organizaciones y usuarios no han aplicado los parches correspondientes o siguen utilizando dispositivos obsoletos. Esta falta de actualización continua exponiendo estos dispositivos a ataques, los cuales han sido recientemente confirmados como activos por la CISA a través de su catálogo KEV (Known Exploited Vulnerabilities).

V. IMPACTO

Los productos y versiones afectados son los siguientes:

Producto	Versiones Afectadas	Vulnerabilidad
D-Link DCS-2530L (Cámara)	Firmware ≤ 1.05.05	CVE-2020-25078, CVE-2020-25079
D-Link DCS-2670L (Cámara)	Firmware ≤ 2.02	CVE-2020-25078, CVE-2020-25079
D-Link DNR-322L (Grabador de red)	Todas las versiones (hasta EOL)	CVE-2022-40799

Tabla 1.- Productos y Versiones afectadas - Vulnerabilidades en Dispositivos D-Link (modelos DCS-2530L, DCS-2670L y DNR -322L)

VI. INDICADORES DE COMPROMISO

Actualmente no se han publicado Indicadores de Compromiso (IoCs) específicos y verificados para las vulnerabilidades CVE-2020-25078 y CVE-2020-25079 relacionadas con las cámaras D-Link DCS-2530L y DCS-2670L.

Ni la CISA, ni D-Link, ni las principales fuentes de ciberseguridad han divulgado hashes, IPs maliciosas, dominios, o rutas específicas que puedan usarse como IoCs concretos para detección automatizada.

VII. RECOMENDACIONES:

- Actualizar a la última versión de firmware disponible.
- Reemplazar dispositivos que han alcanzado fin de vida útil (EOL).
- Restringir acceso a la interfaz de administración desde internet.
- Monitorizar tráfico y eventos de red asociados a los dispositivos.
- Usar contraseñas fuertes y autenticación adicional si es posible.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

CISA (2025). CISA Adds Three Known Exploited Vulnerabilities to Catalog. https://www.cisa.gov/news-events/alerts/2025/08/05/cisa-adds-three-known-exploited-vulnerabilities-catalog

SCYSCAN (2025). CISA Adds 3 D-Link Vulnerabilities to KEV Catalog Amid Active Exploitation Evidence. https://www.scyscan.com/news/cisa-adds-3-d-link-vulnerabilities-to-kev-catalog-amid-active-exploitation-evidence/

SCYSCAN (2025). CISA Adds 3 D-Link Router Flaws to KEV Catalog After Active Exploitation Reports. https://www.scyscan.com/news/cisa-adds-3-d-link-router-flaws-to-kev-catalog-after-active-exploitation-reports/

THE HACKER NEWS (2025). CISA Adds 3 D-Link Router Flaws to KEV Catalog. https://thehackernews.com/2025/08/cisa-adds-3-d-link-router-flaws-to-kev.html

FREEDOM CODER (2025). CVE-2020-25078 – D-Link DCS-2530L and DCS-2670L Devices Unspecified Vulnerability. https://dev.to/freedom_coder/cve-2020-25078-d-link-dcs-2530l-and-dcs-2670l-devices-unspecified-vulnerability-563g