Nro. Alerta:	AL-2025-034	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	14-jul-2025	Vulnerabilidad en D-Link DIR-825 2.10 (CVE-2025-7206)	Pág.: **1** of **6**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Ejecución remota de código (RCE)
Nivel de riesgo: Alta

II. ALERTA

Figura 1. Vulnerabilidad en D-Link DIR-825 2.10 (CVE-2025-7206) - Figura referencial

Nueva vulnerabilidad critica conocida como CVE-2025-7206 de 0-click en router D-link permite a los atacantes remotos sin autenticar, colapsar el servidor Web HTTP del dispositivo, mediante el desbordamiento de búfer basado en pila.

III. INTRODUCCIÓN

Esta vulnerabilidad afecta al router D-link modelo DIR-825 Rev.B con firmware v2.10 y posiblemente versiones inferiores, el defecto reside en el binario httpd (servidor web del router) específicamente la función sub_410DDC, se deriva en un manejo inadecuado del parámetro de "language" en el endpoint de interrupt.language.cgi, con lo que al enviar un valor excesivamente largo al campo “language” mediante una petición HTTP POST desborda la memoria NVRAM del dispositivo ocasionando la sobre escritura de la pila y desencadenando un fallo de segmentación que derriba el servicio.

A dicha vulnerabilidad CVE-2025-7206 se asocia dos (2) CWE:

CWE-121: Desbordamiento de búfer basado en pila, ocurre cuando un programa escribe más datos de los que puede almacenar en un buffer (espacio de memoria reservado) ubicado en la pila (stack), sobrescribiendo direcciones de memoria adyacentes, incluida la dirección de retorno. Esto puede permitir a un atacante ejecutar código malicioso o alterar el flujo del programa.

CWE-119: Restricción inadecuada de operaciones dentro de los límites de un búfer de memoria, se refiere a fallos en la gestión de buffers de memoria que permiten a un atacante leer, modificar o ejecutar código fuera de los límites asignados, lo que puede llevar a:

- Corrupción de memoria
- Ejecución de código arbitrario
- Fugas de información
- Denegación de servicio (DoS)

IV. VECTOR DE ATAQUE

El CVSS 3.1 asigna una puntuación de 9.8 (Crítico) de tipo Red: AV:**N**/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

Se detalla el proceso de colapso del servidor Web de acceso a router D-Link.

Inicia con la carga del httpd del router dlink.

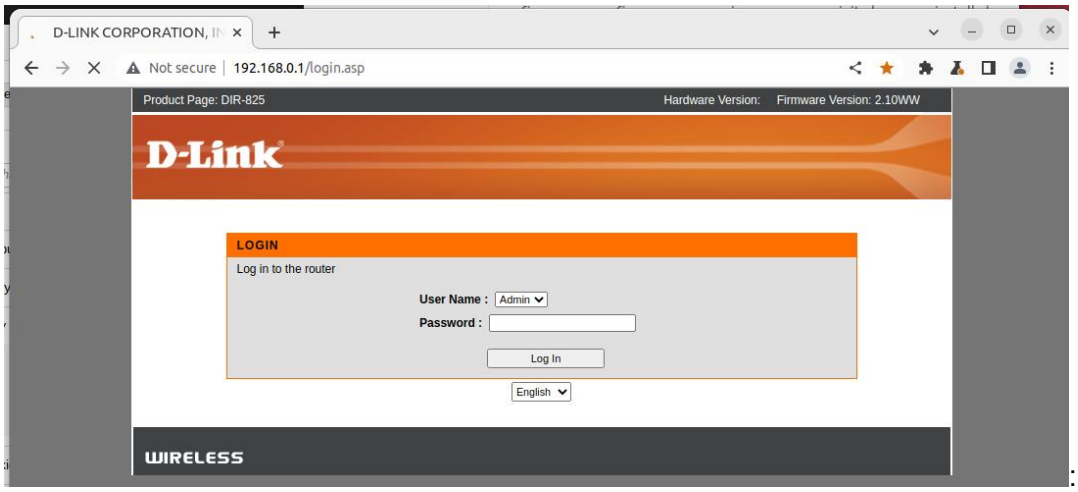

Figura 2. Servidor Web HTTP (httpd) - Vulnerabilidad en D-Link DIR-825 2.10 (CVE-2025-7206)

Dentro del script switch_language.cgi que es el encargado de ejecutar acciones cuando interactúas con la interfaz (cambiar idioma, aplicar configuraciones, reiniciar, etc) yace el defecto en la función sub_410DDC en el campo language, cuando se realiza un HTTP POST a este script, el parámetro language se escribe en la NVRAM para almacenamiento persistente.

```
int sub_410DDC(int a1, char *language) {
    // Unsafe copy of user-supplied language into fixed-size stack buffer
    strcpy(stack_buffer, language);
    nvram_set("language", stack_buffer);
    return 0;
}
```

Figura 3. Función sub_410DDC - Vulnerabilidad en D-Link DIR-825 2.10 (CVE-2025-7206)

Una vez que se guarda la entrada NVRAM desbordada, cualquier solicitud posterior a una página ASP front-end (ej. login.asp) activa la carga dinámica de un archivo JavaScript de idioma correspondiente. La página incluye.

```
<script type="text/javascript" src="lang_<% CmoGetCfg("language","none");
%>.js"></script>
```

Figura 4. Llamado archivo Javascript - Vulnerabilidad en D-Link DIR-825 2.10 (CVE-2025-7206)

El valor esperado de regreso es el idioma del archivo, lang_es.js o lang_en.js en el caso de un desbordamiento de buffer ocasionado por el atacante, podría pasar el campo languaje como por ejemplo:

```
<script src="lang_../../../../etc/passwd.js"></script>
```

Figura 5. Valor erróneo generado por desbordamiento de búfer. - Vulnerabilidad en D-Link DIR-825 2.10 (CVE-2025-7206)

Durante el análisis, httpd entra en la ruta do_ebd_js, terminando por llamar a nvram_get("language").

La cadena devuelta pasa por una serie compleja de funciones internas - sub_40BFC4 (función o subrutina dentro del firmware de un dispositivo D-Link, identificable al analizar el código ensamblador o binario descompilado del firmware) - donde otra concatenación insegura escribe más allá del búfer designado, provocando finalmente un fallo de segmentación que colapsa el servicio.

Con Prueba de Concepto (PoC): La PoC mínimo demuestra el fallo en dos pasos. Primero, establecer el valor de lenguaje sobredimensionado mediante switch_language.cgi:

```
POST /switch_language.cgi HTTP/1.1
Host: 192.168.0.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 200
Connection: close

html_response_lang=login.asp&language=AAAA…(over 200 bytes)…AAAA&site=es
```

Figura 6. Cabecera de método POST - Vulnerabilidad en D-Link DIR-825 2.10 (CVE-2025-7206)

Inmediatamente después, una simple solicitud GET a cualquier página ASP desencadena el desbordamiento:

```
GET /login.asp HTTP/1.1
Host: 192.168.0.1
Connection: close
```

Figura 7. Cierre de conexión tras cualquier envió de petición GET - Vulnerabilidad en D-Link DIR-825 2.10 (CVE-2025-7206)

La entrada NVRAM excesivamente larga corrompe la pila (stack) durante la ejecución de sub_40BFC4, provocando el cierre inmediato del proceso httpd sin requerir autenticación ni acción explícita del usuario.

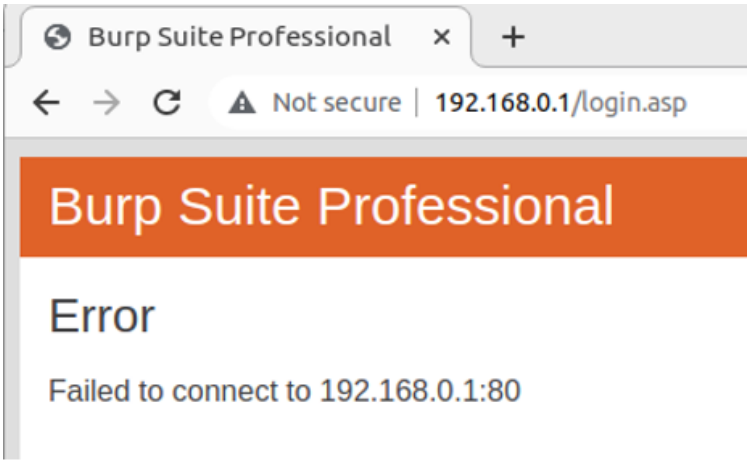

Figura 8. Colapso del servidor HTTP - Vulnerabilidad en D-Link DIR-825 2.10 (CVE-2025-7206)

V. IMPACTO

Producto: D-Link modelo DIR-825 Rev. B - Firmware versión 2.10 (y posiblemente versiones anteriores de firmware para Rev.B) lo que con lleva un alto impacto también en:

- **Ejecución remota de código (RCE):** El principal impacto de esta vulnerabilidad es la posibilidad de que un atacante remoto ejecute código arbitrario en el dispositivo afectado. Esto otorga al actor malicioso control total sobre el enrutador, lo que habilita la instalación de puertas traseras, la manipulación del firmware o la alteración del tráfico de red para propósitos maliciosos.

- **Red interna comprometida:** Una vez que el enrutador ha sido comprometido, el atacante puede interceptar, redirigir o manipular el tráfico que fluye a través del dispositivo. Esto abre la puerta al robo de credenciales, la captura de información confidencial, y el acceso no autorizado a sistemas internos, lo que representa un riesgo serio para la confidencialidad e integridad de la red organizacional.

- **Mayor riesgo de propagación de malware:** El control del dispositivo vulnerable puede permitir al atacante utilizarlo como una base para movimientos laterales dentro de la red o como punto de partida para lanzar nuevos ataques contra otros activos conectados. Además, podría aprovecharse como canal para distribuir malware a través de la red local, incrementando exponencialmente el impacto del incidente inicial.

VI. INDICADORES DE COMPROMISO

Sitio web del servidor HTTP default http[:]192.168.0.1/login.asp

VII. RECOMENDACIONES:

- Aislar y/o reemplazar los dispositivos afectados, ya que el modelo DIR825 v2.10 se encuentra fuera de soporte.
- Desactivar el acceso remoto al panel de administración web (puertos 80/443).
- Implementar filtrado IP o VPN para restringir el acceso de administración solo a direcciones confiables.
- Monitorear tráfico saliente del router en busca de conexiones a dominios o IPs inusuales.

- Actualizar políticas de inventario para identificar y retirar equipos obsoletos o sin soporte de seguridad.
- Aplicar segmentación de red para evitar que un router comprometido pueda afectar a sistemas críticos.
- Actualizar firmas de detección en IDS/IPS o antivirus para reconocer intentos de explotación del CGI vulnerable.

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:

SECURITYVULNERABILITY.IO (2025). Vulnerability Details: CVE-2025-7206. https://securityvulnerability.io/vulnerability/CVE-2025-7206

GBHACKERS (2025). Critical D-Link Vulnerability. https://gbhackers.com/critical-d-link-vulnerability/

CYBERSECURITY NEWS (2025). D-Link 0-Click Vulnerability. https://cybersecuritynews.com/d-link-0-click-vulnerability/

TEAMWIN (2025). Critical D-Link 0-Click Vulnerability Allows Remote Attackers to Crash the Server. https://teamwin.in/critical-d-link-0-click-vulnerability-allows-remote-attackers-to-crash-the-server/

INCIBE-CERT (2025). CVE-2025-7206. https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2025-7206

MITRE (2025). CWE-121: Stack-Based Buffer Overflow. https://cwe.mitre.org/data/definitions/121.html