

# ALERTA INTEGRADA DE SEGURIDAD DIGITAL



La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.


El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

## Contenido

CVE-2026-41940 – Autenticación omitida en cPanel & WHM .....	4
Vulnerabilidad en dispositivos de Moza. ....	6
Vulnerabilidad crítica en D-Link DI-8100. ....	7
Índice alfabético .....	8

 Centro Nacional de Seguridad Digital	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 062</b>		Fecha: 30-04-2026
			Página: 4 de 8
<b>Componente que reporta</b>	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
<b>Nombre de la alerta</b>	CVE-2026-41940 – Autenticación omitida en cPanel & WHM		
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	EVC
<b>Medios de propagación</b>	Red, Internet		
<b>Código de familia</b>	H	<b>Código de Sub familia</b>	H01
<b>Clasificación temática familia</b>	Intento de intrusión		

**Descripción**

**1. ANTECEDENTES:**


El 29 de abril de 2026 se publicó la vulnerabilidad crítica CVE-2026-41940, que afecta a cPanel y WHM (incluido WP Squared) en múltiples versiones mantenidas históricamente. El fallo corresponde a un control de autenticación ausente (CWE-306) dentro del flujo de inicio de sesión, lo que permite a atacantes remotos no autenticados obtener acceso indebido al panel de control. La severidad es CRÍTICA (CVSS v3.1 9.8; CVSS v4.0 9.3) y la vulnerabilidad fue incluida en el Catálogo KEV de CISA, confirmando explotación activa y priorización de mitigación inmediata para infraestructuras expuestas.

**Métrica**

Versión CVSS 4.0
Versión CVSS 3.x
Versión CVSS 2.0

Los esfuerzos de enriquecimiento de NVD hacen referencia a información disponible públicamente para asociar cadenas vectoriales. También se muestra información CVSS aportada por otras fuentes.

**Cadenas de gravedad y vector CVSS 3.x:**


**CNA:** VulnCheck

**Puntuación base:**
**9.8 CRÍTICO**

**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

*Ilustración 1 CVE-2026-41940 – Autenticación omitida en cPanel & WHM.*

**2. DETALLES:**

La vulnerabilidad permite omitir el proceso normal de autenticación en el inicio de sesión de cPanel/WHM, habilitando acceso no autorizado desde la red sin necesidad de credenciales (AV:N, PR:N, UI:N). El impacto es crítico, ya que compromete de manera completa la confidencialidad, integridad y disponibilidad del sistema, y existe código público de explotación que puede encadenarse hasta escenarios de ejecución remota de código (RCE).

El fallo afecta a un amplio rango de versiones de cPanel/WHM, desde la 11.40 hasta ramas recientes previas a los parches de seguridad, así como a WP Squared en versiones no corregidas. Debido al rol central de estas plataformas en entornos de hosting, el riesgo se amplifica considerablemente, pudiendo derivar en la toma total de control del servidor, manipulación de cuentas, despliegue de malware y el compromiso simultáneo de múltiples sitios web alojados.





### 3. RECOMENDACIONES:

- Actualizar de inmediato a las versiones parcheadas indicadas por el proveedor (cPanel/WHM y WP Squared) y reiniciar servicios donde aplique.
- Restringir el acceso al panel (WHM/cPanel) mediante allowlists de IP, VPN o redes administrativas mientras se valida la corrección.
- Supervisar indicios de compromiso: revisión de logs de autenticación, cambios de cuentas, tareas cron, binarios sospechosos y web shells.
- Aplicar hardening: habilitar WAF, MFA (si está soportado), desactivar endpoints no necesarios y reducir exposición a Internet.
- Inventariar instancias afectadas (hosting, VPS, dedicados) y priorizar aquellas con exposición pública.
- Alinear respuesta a ISO/IEC 27035: registrar el incidente, preservar evidencia y ejecutar análisis post-incidente.
- Seguir la guía de CISA (KEV) y completar mitigaciones dentro del plazo recomendado; si no es posible, aislar o retirar el servicio

**Fuente de Información:**

- <https://nvd.nist.gov/vuln/detail/CVE-2026-41940>

	<b>ALERTA DE SEGURIDAD DIGITAL N°237</b>			Fecha: 30-04-2026
				Página: 6 de 8
<b>Componente que reporta</b>	<b>DIRECCIÓN NACIONAL DE INTELIGENCIA</b>			
<b>Nombre de la alerta</b>	Vulnerabilidad en dispositivos de Moza.			
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	EVC	
<b>Medios de propagación</b>	Red, Internet			
<b>Código de familia</b>	H	<b>Código de Sub familia</b>	H01	
<b>Clasificación temática familia</b>	Intento de intrusión			
<b>Descripción</b>				
<p><b>1. ANTECEDENTES:</b></p> <p>Moza Inc. ha publicado una vulnerabilidad de severidad <b>MEDIA</b> clasificada como CWE-282: Gestión inadecuada de la propiedad que afecta a los routers de las series Moxa EDR-G9010 y EDR-8010. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante obtener información confidencial.</p> <p><b>2. DETALLES:</b></p> <p>La vulnerabilidad de severidad <b>media</b> identificada por MITRE como <a href="#">CVE-2026-3867</a> de tipo CWE-282: Gestión inadecuada de la propiedad que afecta a los routers de las series Moxa EDR-G9010 y EDR-8010, podría permitir atacante obtener información confidencial. La explotación solo es posible bajo una condición específica: cuando el archivo de configuración se ha exportado. Esta vulnerabilidad no afecta la integridad ni la disponibilidad del producto afectado, y no se ha identificado ningún impacto en la confidencialidad, la integridad o la disponibilidad del sistema posterior.</p> <p>Esta vulnerabilidad no afecta la integridad ni la disponibilidad del producto afectado, y no se ha identificado ningún impacto en la confidencialidad, la integridad o la disponibilidad del sistema posterior.</p> <p><b>A. Productos afectados:</b></p> <ul style="list-style-type: none"> <li>– Moxa EDR-G9010 (todas las versiones),</li> <li>– Moxa EDR-8010 (todas las versiones).</li> </ul> <p><b>3. RECOMENDACIONES:</b></p> <ul style="list-style-type: none"> <li>• Aplicar el parche proporcionado por Moxa en su advisory de seguridad (MPSA-261521).</li> <li>• Evitar exportar archivos de configuración innecesarios y restringir privilegios de usuarios autenticados.</li> </ul>				
<b>Fuente de Información:</b>		<ul style="list-style-type: none"> <li>• <a href="https://www.moxa.com/en/support/product-support/security-advisory/mpsa-261521-cve-2026-3867-cve-2026-3868-improper-ownership-management-and-improper-handling-of-length-parameter-incons">hxxps[:]//www.moxa.com/en/support/product-support/security-advisory/mpsa-261521-cve-2026-3867-cve-2026-3868-improper-ownership-management-and-improper-handling-of-length-parameter-incons</a></li> </ul>		

	<b>ALERTA DE SEGURIDAD DIGITAL N°238</b>		Fecha: 30-04-2026
			Página: 7 de 8
<b>Componente que reporta</b>	<b>DIRECCIÓN NACIONAL DE INTELIGENCIA</b>		
<b>Nombre de la alerta</b>	Vulnerabilidad crítica en D-Link DI-8100.		
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	EVC
<b>Medios de propagación</b>	Red, Internet		
<b>Código de familia</b>	H	<b>Código de Sub familia</b>	H01
<b>Clasificación temática familia</b>	Intento de intrusión		
<b>Descripción</b>			
<p><b>1. ANTECEDENTES:</b></p> <p>D-Link ha reportado una vulnerabilidad de severidad <b>“CRÍTICA”</b> clasificada como CWE-119 / CWE-120: Restricción incorrecta de operaciones dentro de los límites de un búfer / desbordamiento clásico de búfer que afecta al dispositivo D-Link DI-8100 (versión 16.07.26A1). Esta vulnerabilidad permite la ejecución remota de código o la interrupción completa del sistema, comprometiendo la confidencialidad, integridad y disponibilidad del dispositivo. El riesgo es elevado debido a que puede ser explotada sin autenticación previa y a través de la red, lo que la convierte en un vector crítico para ataques dirigidos contra infraestructuras que utilicen este equipo.</p> <p><b>2. DETALLES:</b></p> <p>La vulnerabilidad de severidad <b>crítica</b> identificada por MITRE como <a href="#">CVE-2026-7248</a> se origina en la función tgfile_htm dentro del archivo tgfile.htm, perteneciente al componente CGI del dispositivo. El fallo se produce cuando un atacante manipula el parámetro fn, provocando un desbordamiento de búfer al no existir una validación adecuada del tamaño de entrada. Este tipo de error permite sobrescribir memoria adyacente, lo que puede derivar en ejecución de código arbitrario.</p> <p>El desbordamiento de búfer permite a un atacante sobrescribir regiones de memoria, lo que puede derivar en ejecución de código arbitrario con privilegios del proceso afectado. En dispositivos de red como routers, esto puede traducirse en control total del dispositivo, interceptación de tráfico o pivoting hacia redes internas.</p> <p>En el caso de CVE-2026-7248, la explotación puede realizarse de forma remota (AV:N) y sin autenticación (PR:N), lo que reduce significativamente la complejidad del ataque. La vulnerabilidad presenta impacto alto en confidencialidad, integridad y disponibilidad (C:H/I:H/A:H), lo que indica que un atacante podría tomar control total del dispositivo afectado o inutilizarlo mediante ataques de denegación de servicio.</p> <p>Respecto a la explotación, existe evidencia de que el exploit ha sido divulgado públicamente (PoC disponible), lo que incrementa el riesgo de explotación activa. Sin embargo, no puedo confirmar la atribución a un actor de amenaza específico ni campañas activas con base en fuentes verificables actuales. La disponibilidad pública del exploit implica que actores oportunistas podrían incorporarlo rápidamente en campañas automatizadas.</p> <p><b>A. Productos afectados:</b></p> <ul style="list-style-type: none"> <li>– D-Link DI-8100, versión: 16.07.26A1.</li> </ul> <p><b>3. RECOMENDACIONES:</b></p> <ul style="list-style-type: none"> <li>• Aplicar actualizaciones o parches oficiales del fabricante tan pronto estén disponibles.</li> <li>• Restringir el acceso al endpoint CGI vulnerable mediante ACLs o segmentación de red.</li> <li>• Implementar controles de firewall para limitar acceso externo al dispositivo.</li> <li>• Deshabilitar interfaces de administración expuestas a Internet.</li> <li>• Monitorear tráfico anómalo hacia rutas CGI, especialmente parámetros manipulados (fn).</li> <li>• Implementar IDS/IPS con firmas para detectar intentos de buffer overflow en dispositivos IoT.</li> </ul>			
<b>Fuente de Información:</b>	<ul style="list-style-type: none"> <li>• <a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-traversal-8bYndVrZ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-traversal-8bYndVrZ</a></li> </ul>		

## Índice alfabético

Explotación de vulnerabilidades conocidas .....4,6,7