PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

140-2025-CNSD

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 Aéreadel 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 lasempresas 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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°140	Fecha: 17-06-2025
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Suplantaciones de perfiles en redes sociales		
Tipo de Ataque	Suplantación	Abreviatura	Suplantación
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G02
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

El uso de las redes sociales se ha convertido en una actividad cotidiana que muchas veces se realiza sin tener en cuenta las consecuencias que derivan de su uso. El elevado número de usuarios que existe en estas plataformas y la facilidad con la que éstos publican fotografías o comparten información sensible, como ubicaciones, hace que cada vez sea más frecuente estar expuestos a riesgos de seguridad y privacidad.

2. DETALLES:

El oversharing o sobreexposición de nuestra información personal puede ser aprovechada por usuarios malintencionados que buscan suplantar la identidad de los usuarios de la red.

La suplantación de identidad ocurre cuando alguien crea un perfil falso o secuestra una cuenta real para hacerse pasar por otra persona. La suplantación de perfiles en redes sociales se encuentra entre los delitos digitales más reportados en los últimos dos años. La facilidad con la que se puede copiar una imagen de perfil, construir una biografía falsa o incluso tomar el control de una cuenta legítima ha hecho que este tipo de fraude se multiplique.

Las motivaciones detrás de la suplantación son múltiples. En algunos casos, el objetivo es robar información personal para cometer fraudes financieros. También engañar a amigos o familiares y pedir dinero a través de mensajes directos.

En otros, se trata de dañar la imagen pública de una persona o empresa, incluso, las víctimas pueden ver comprometidos sus datos bancarios, relaciones personales o incluso su seguridad física si la información difundida por el impostor se usa para extorsión o acoso. Ello está asociado con la comisión de delitos que atentan contra el honor, la intimidad y la propia imagen de los otros usuarios de la red.

Tipos de suplantación de identidad en redes sociales:

- **Acceso a la cuenta de un usuario:** Una vez dentro, el ladrón puede enviar mensajes privados, publicar contenido y compartir opiniones en la red. Además, puede enviar enlaces fraudulentos a otros usuarios, acceder a su cuenta bancaria e incluso realizar compras online.
- **Creación un perfil falso con los datos de la víctima suplantada:** el atacante utiliza la información personal y las fotos de una persona real para abrir una nueva cuenta en una red social. El perfil parece real y, por tanto, los usuarios no se dan cuenta de que existe una suplantación de identidad.

3. RECOMENDACIONES:

- Utilizar contraseñas robustas y cambiarlas periódicamente.
- Activar la autenticación en dos pasos en todas las redes sociales.
- Limitar la visibilidad de la información personal, como número de teléfono, dirección de correo o ubicación.
- Revisar las solicitudes de amistad y no aceptar perfiles desconocidos sin verificar su autenticidad.
- Supervisar regularmente tu nombre en buscadores y redes para detectar posibles cuentas que se hagan pasar por ti.
- Guardar evidencia como capturas de pantalla, mensajes enviados por el impostor y enlaces al perfil falso, en caso se haya detectado que alguien ha creado un perfil falso.

Fuente de Información:	• hxxps://www.infobae.com/tecno/2025/06/17/suplantaciones-de-perfiles-en-redes-sociales-asi-debes-actuar-para-evitar-ser-presa-de-ciberdelincuentes/ • hxxps://www.mobbeel.com/blog/suplantacion-identidad-redes-sociales/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°140	Fecha: 17-06-2025 Página: 5 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades en Microsoft Edge		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Microsoft corporation ha publicado dos vulnerabilidades de severidad **CRÍTICA** de tipo uso después de la liberación y confusión de tipos que afectan a Microsoft Edge (basado en Chromium). La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado la ejecución de código arbitrario.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-5958 de tipo uso después de la liberación en Microsoft Edge (basado en Chromium), podría permitir a un atacante remoto explotar la corrupción del montón engañando al usuario para que visite una página HTML especialmente diseñada. Una explotación exitosa podría provocar la ejecución de código arbitrario, con riesgos significativos para la confidencialidad, la integridad y la disponibilidad del sistema afectado.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-5959 de tipo confusión de tipos en el motor JavaScript V8 de Google Chrome en plataforma Windows, Mac y Linux, podría permitir un atacante remoto ejecute código arbitrario dentro del entorno de pruebas del navegador. Aunque el código se ejecuta dentro del entorno de pruebas, puede comprometer la seguridad del navegador y los datos del usuario. No se requiere privilegios especiales ni interacción del usuario más allá de visitar una página web maliciosa, la explotación exitosa permite la ejecución de código arbitrario en el contexto del navegador, lo que puede conducir al robo de datos, secuestro de sesiones o mayor explotación si se combina con otras vulnerabilidades.

A. Productos afectados:

- Google Chrome, versiones anteriores a 137.0.7151.103 en Windows, Mac y Linux.
- Microsoft Edge, versiones anteriores a 137.0.3296.83.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-5958 • hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-5959

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°140	Fecha: 17-06-2025
		Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de comandos en puntos de acceso de Hikvision		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Hangzhou Hikvision Digital Technology Co., Ltd. ha publicado una vulnerabilidad de severidad **ALTA** de tipo validación de entrada incorrecta que afecta a varios modelos de puntos de acceso inalámbricos de Hikvision. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución remota de comandos debido a una validación de entrada insuficiente.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-39240 de tipo validación de entrada incorrecta que afecta a varios modelos de puntos de acceso inalámbricos de Hikvision. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución remota de comandos debido a una validación de entrada insuficiente.

Los atacantes con credenciales válidas pueden explotar esta vulnerabilidad enviando paquetes manipulados con comandos maliciosos a los dispositivos afectados, lo que provoca la ejecución arbitraria de comandos.

A. Productos afectados:

- DS-3WAP622G-SI, V1.1.5402 build241014 (E2254P02) y las versiones anteriores.
- DS-3WAP623E-SI, V1.1.5400 build240814 (E2254) y las versiones anteriores.
- DS-3WAP521-SI, V1.1.5400 build240814 (E2254) y las versiones anteriores.
- DS-3WAP522-SI, V1.1.5402 build241014 (E2254P02) y las versiones anteriores.
- DS-3WAP621E-SI, V1.1.5400 build240814 (E2254) y las versiones anteriores.
- DS-3WAP622E-SI, V1.1.5402 build241014 (E2254P02) y las versiones anteriores.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.

Fuente de Información:	• hxxps://www.hikvision.com/en/support/cybersecurity/security-advisory/remote-command-execution-vulnerability-in-some-hikvision-wireless-access-point/ • hxxps://www.hikvision.com/en/support/download/firmware/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°140	Fecha: 17-06-2025 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en enrutadores TP-Link		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

TP-Link Technologies CO. LTD ha publicado una vulnerabilidad de severidad **ALTA** de tipo inyección de comandos que afecta a múltiples routers inalámbricos TP-Link. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución remota de código en el sistema objetivo.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2023-33538 de tipo inyección de comandos a través del componente /userRpm/WlanNetworkRpm, podría permitir a un atacante remoto no autenticado la ejecución remota de código en el sistema objetivo.

La vulnerabilidad existe en el componente /userRpm/WlanNetworkRpm y puede explotarse mediante el parámetro ssid1 en una solicitud HTTP GET especialmente diseñada, lo que permite a un atacante ejecutar comandos arbitrarios del sistema en el dispositivo.

Esta vulnerabilidad viene siendo explotado activamente en la naturaleza.

TP-Link, indicó que el soporte oficial para los tres modelos de routers vulnerables ha finalizado y ya no recibiera actualizaciones y parches de seguridad.

A. Productos afectados:

- TP-Link TL-WR740N V1/V2.
- TP-Link TL-WR841N V8/V10.
- TP-Link TL-WR940N V2/V4.

3. RECOMENDACIONES:

- Suspender el uso de los productos afectados, ya que los productos afectados podrían haber llegado al final de su vida útil (EoL) o al final de su servicio (EoS).
- Supervisar la actividad de la red y del dispositivo para detectar cualquier comportamiento anómalo que pueda indicar intentos de explotación.
- Limitar la exposición de los dispositivos afectados restringiendo el acceso a las interfaces de administración, por ejemplo, aislándolos de redes no confiables o deshabilitando la administración remota cuando sea posible.

Fuente de Información:	• hxxps://web.archive.org/web/20230609111043/https://github.com/a101e-IoTvul/iotvul/blob/main/tp-link/3/TL-WR940N_TL-WR841N_userRpm_WlanNetworkRpm_Command_Injection.md • hxxps://www.tp-link.com/nordic/support/faq/3562/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°140	Fecha: 17-06-2025 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en Google Chrome		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha publicado dos vulnerabilidades de severidad **ALTA** de tipo desbordamiento de enteros y uso posterior a la liberación que afectan al componente V8 de Google Chrome. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-6191 de tipo desbordamiento de enteros en el componente V8 de Google Chrome, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un desbordamiento de enteros en el componente V8 de Google Chrome. Un atacante remoto puede engañar a la víctima para que abra una página web especialmente diseñada, provocar un desbordamiento de enteros y ejecutar código arbitrario en el sistema objetivo.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-6192 de tipo uso posterior a la liberación en el componente V8 de Google Chrome, podría permitir que un atacante remoto comprometa el sistema vulnerable. La vulnerabilidad existe debido a un error de uso tras liberación en el componente Profiler de Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, generar un error de uso tras liberación y ejecutar código arbitrario en el sistema objetivo.

La explotación exitosa de estas vulnerabilidades podría permitir a un atacante comprometer el sistema vulnerable.

A. Productos afectados:

- Google Chrome: 120.0.6099.62 - 137.0.7151.104.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_17.htmlxxx • hxxps://crbug.com/420697404 • hxxps://crbug.com/421471016

Índice alfabético