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

106-2025-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°106	Fecha: 07-05-2025
		Página: 4 de 11

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Convencen a la IA para robar contraseñas		
Tipo de Ataque	Robo de información	Abreviatura	RobInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K01
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

Hacer uso de la inteligencia artificial se está volviendo cada vez más común en diferentes áreas, igualmente en la informática, donde ya está evolucionando a la creación y edición de código de programación, lo cual puede ser un problema de ciberseguridad.

2. DETALLES:

Se supone que todos los chatbots oficiales cuentan con sistemas de seguridad y garantizan la protección de los usuarios. Sin embargo, los ciberdelincuentes no se cansan de buscar nuevas maneras de conseguir víctimas y parece que esta será uno de los métodos más usados en los próximos años.

Los expertos han reportado que los modelos pueden ser engañados a través de comandos cuidadosamente diseñados conocidos como prompts, induciendo a ciertos modelos de lenguaje a producir resultados con implicaciones peligrosas, como la creación de malware o el robo de contraseñas.

De esta manera, usando frases específicas y una estructura diferente a lo convencional se logra que el asistente virtual arroje resultados que pueden llegar a ser ilegales.

Incluso usando herramientas comunes como ChatGPT, DeepSeek y Claude, se han logrado generar instrucciones completas para el desarrollo de virus informáticos, simplemente utilizando estructuras narrativas cuidadosamente redactadas, burlando así los sistemas de limitaciones de seguridad.

Una de las razones por las cuales este escenario es especialmente alarmante es que las herramientas utilizadas están disponibles de forma pública, por lo que se espera un aumento en los ataques de phishing, ya que la IA facilita la creación de páginas falsas, correos apócrifos y documentos digitales que imitan de manera casi perfecta a entidades legítimas.

La barrera de entrada para la ciberdelincuencia se reduce drásticamente, abriendo un camino para que individuos sin formación técnica puedan, con el prompt adecuado, generar software malicioso en cuestión de minutos.

3. RECOMENDACIONES:

- Evitar almacenar contraseñas en lugares accesibles.
- Limpiar las cookies del navegador de forma recurrente.
- Utilizar gestores de contraseñas que generen credenciales robustas.

Fuente de Información:	• hxxps://computerhoy.20minutos.es/tecnologia/convencen-ia-robar-contrasenas-hackers-foros-clandestinos-ni-saber-programar-cualquiera-puede-hacerlo-1459596?utm_source=Threads&utm_medium=social&utm_campaign=CH • hxxps://www.infobae.com/tecno/2025/05/07/la-ia-ya-puede-hackear-expertos-advierten-sobre-virus-creados-con-simples-prompts/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°106	Fecha: 07-05-2025 Página: 5 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el plugin ContentStudio para WordPress		
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 una vulnerabilidad de severidad **MEDIA** de tipo falta de autorización que afecta al plugin ContentStudio para WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario no autorizado explotar el sistema omitiendo las comprobaciones de autorización.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-47692 de tipo falta de autorización, podría permitir a un usuario no autorizado explotar el sistema omitiendo las comprobaciones de autorización. La vulnerabilidad de control de acceso permite la omisión de las comprobaciones de autorización (fuente propia inferida, ya que no aparece en los resultados de búsqueda).

A. Productos afectados:

- Plugin ContentStudio para WordPress, todas las versiones hasta la 1.3.3.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//patchstack[.]com/database/wordpress/plugin/contentstudio/vulnerability/wordpress-contentstudio-1-3-3-broken-access-control-vulnerability?_s_id=cve

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°106	Fecha: 07-05-2025 Página: 6 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en productos Apache		
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:

Apache Foundation ha publicado una vulnerabilidad de severidad **MEDIA** de tipo asignación de memoria con un valor de tamaño excesivo que afecta la gestión de memoria durante la deserialización en Apache ActiveMQ. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario no autorizado explotar el sistema omitiendo las comprobaciones de autorización.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-27533 de tipo asignación de memoria con un valor de tamaño excesivo, podría permitir a un usuario no autorizado explotar el sistema omitiendo las comprobaciones de autorización.

Esta falla se produce durante la desagrupación de comandos OpenWire, donde el valor de tamaño de los búferes puede manipularse para provocar una asignación de memoria incorrecta, lo que podría provocar una denegación de servicio u otros impactos.

A. Productos afectados:

- Apache ActiveMQ 6.0.0 anterior a 6.1.6.
- Apache ActiveMQ 5.18.0 anterior a 5.18.7.
- Apache ActiveMQ 5.17.0 anterior a 5.17.7.
- Apache ActiveMQ 5.16.0 anterior a 5.16.8.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//lists[.]apache[.]org/thread/8hcm25vf7mchg4zbbhnlx2lc5bs705h

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°106	Fecha: 07-05-2025 Página: 7 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en complemento para WordPress		
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 una vulnerabilidad de severidad **MEDIA** de tipo falsificación de solicitud del lado del servidor (SSRF) que afecta al plugin de WordPress llamado Activity Link Preview para BuddyPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante manipular las solicitudes del lado del servidor, lo que podría provocar acceso no autorizado o divulgación de información mediante solicitudes manipuladas.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-47548 de tipo falsificación de solicitud del lado del servidor (SSRF), podría permitir a un atacante manipular las solicitudes del lado del servidor, lo que podría provocar acceso no autorizado o divulgación de información mediante solicitudes manipuladas.

Las vulnerabilidades SSRF normalmente permiten a los atacantes hacer que el servidor realice solicitudes no deseadas, que pueden usarse para acceder a sistemas internos o datos confidenciales.

A. Productos afectados:

- Wbcom Designs - Activity Link Preview para BuddyPress versiones hasta la 1.4.4.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//patchstack[.]com/database/wordpress/plugin/activity-link-preview-for-buddypress/vulnerability/wordpress-wbcom-designs-activity-link-preview-for-buddypress-1-4-4-server-side-request-forgery-ssrf-vulnerability?_s_id=cve

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°106	Fecha: 07-05-2025 Página: 8 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el software del controlador inalámbrico Cisco IOS XE		
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:

Cisco Systems, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo uso de credenciales codificadas en la función de descarga de imágenes de puntos de acceso (AP) fuera de banda del software Cisco IOS XE para controladores de LAN inalámbrica (WLC). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado cargar archivos arbitrarios en un sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-20188 de tipo uso de credenciales codificadas en la función de descarga de imágenes de puntos de acceso (AP) fuera de banda del software Cisco IOS XE para controladores de LAN inalámbrica (WLC), podría permitir a un atacante remoto no autenticado cargar archivos arbitrarios en un sistema afectado.

Esta vulnerabilidad se debe a la presencia de un token web JSON (JWT) codificado de forma rígida en un sistema afectado. Un atacante podría explotar esta vulnerabilidad enviando solicitudes HTTPS manipuladas a la interfaz de descarga de imágenes de AP. Una explotación exitosa podría permitir al atacante cargar archivos, atravesar rutas y ejecutar comandos arbitrarios con privilegios de root.

Para que la explotación sea exitosa, la función de Descarga de Imágenes de AP fuera de banda debe estar habilitada en el dispositivo. No está habilitada por defecto.

A. Productos afectados:

Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco IOS XE para WLC y tienen habilitada la función de descarga de imágenes de AP fuera de banda:

- Controladores inalámbricos Catalyst 9800-CL para la nube.
- Controlador inalámbrico integrado Catalyst 9800 para conmutadores de las series Catalyst 9300, 9400 y 9500.
- Controladores inalámbricos de la serie Catalyst 9800.
- Controlador inalámbrico integrado en puntos de acceso Catalyst.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.
- Desactivar la función de descarga de imágenes de AP fuera de banda como estrategia de mitigación, en caso que aún no se pueda actualizar a una versión de software corregida. Con esta función desactivada, la descarga de imágenes de AP utilizará el método CAPWAP para la actualización de imágenes de AP, lo cual no afecta el estado del cliente AP.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°106	Fecha: 07-05-2025
		Página: 9 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en BIG-IP		
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:

F5 Networks ha publicado múltiples vulnerabilidades de severidad **MEDIA** de tipo escritura fuera de límites, error de validación de entrada, desbordamiento de búfer, desreferencia de puntero NULL e inyección de comandos del sistema operativo que afectan al Firmware BIG-IP. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado realizar un ataque de denegación de servicio (DoS) y ejecutar comandos arbitrarios del sistema operativo con privilegios elevados.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-41431 de tipo escritura fuera de límites en BIG-IP, podría permitir a un atacante remoto realizar un ataque de DoS. La vulnerabilidad existe debido a un error de límite al configurar la duplicación de conexiones en un servidor virtual. Un atacante remoto puede enviar tráfico especialmente diseñado al dispositivo, activar una escritura fuera de límites y realizar un ataque de DoS.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-35995 de tipo error de validación de entrada en BIG-IP, podría permitir a un atacante remoto realizar un ataque de DoS. La vulnerabilidad existe debido a una validación insuficiente de la entrada proporcionada por el usuario cuando un sistema BIG-IP PEM tiene licencia de categorización de URL y la política de categorización de URL o una iRule con el comando urlcat está habilitada en un servidor virtual. Un atacante remoto puede enviar una entrada especialmente diseñada al sistema y realizar un ataque de DoS.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-36525 de tipo desbordamiento de búfer en BIG-IP, podría permitir a un atacante remoto realizar un ataque de DoS. La vulnerabilidad se debe a un error de límite al configurar un perfil BIG-IP APM PingAccess en un servidor virtual. Un atacante remoto puede enviar tráfico especialmente diseñado al sistema y realizar un ataque de DoS.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-41433 de tipo desreferencia de puntero NULL en BIG-IP, podría permitir a un atacante remoto realizar un ataque de DoS. La vulnerabilidad se debe a un error de desreferencia de puntero nulo cuando se configura un perfil de puerta de enlace de capa de aplicación (ALG) del marco de enrutamiento de mensajes (MRF) del Protocolo de Iniciación de Sesión (SIP) en un servidor virtual de enrutamiento de mensajes. Un atacante remoto puede enviar tráfico especialmente diseñado al sistema y realizar un ataque de DoS.

La vulnerabilidad de severidad **baja** identificada por MITRE como CVE-2025-31664 de tipo inyección de comandos del sistema operativo en BIG-IP, podría permitir a un usuario remoto aumentar los privilegios en el sistema. La vulnerabilidad existe debido a una validación de entrada incorrecta en algunos comandos de iControl REST y BIG-IP TMOS Shell (tmsh). Un usuario remoto con privilegios puede enviar una entrada especialmente diseñada al sistema y ejecutar comandos arbitrarios del sistema operativo con privilegios elevados.

A. Productos afectados:

- BIG-IP PEM: versiones anteriores a 17.1.03.
- BIG-IP: 15.1.0 - 15.1.10.6.0.11.6, 16.1.0 - 16.1.4.3, 17.1.0 - 17.1.1.4.
- BIG-IP: 15.1.0 - 15.1.10.6.0.11.6, 16.1.0 - 16.1.5.2.0.7.5, 17.1.0 - 17.1.2.1.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://my.f5.com/manage/s/article/K000150668 • hxxps://my.f5.com/manage/s/article/K000149952 • hxxps://my.f5.com/manage/s/article/K000150598 • hxxps://my.f5.com/manage/s/article/K000140937 • hxxps://my.f5.com/manage/s/article/K000148591

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°106	Fecha: 07-05-2025
		Página: 10 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en Tenable Security Center		
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 múltiples vulnerabilidades de severidad **CRÍTICA** de tipo complejidad ineficiente de expresiones regulares, desbordamiento de búfer basado en montón y desbordamiento de entero o envoltura en Tenable Security Center. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución remota de código arbitrario y generar un ataque de denegación de servicio (DoS).

2. DETALLES:

Tenable indico que se detectaron múltiples vulnerabilidades en varios componentes de terceros (sqlite, ua-parser-js), y los proveedores han publicado versiones actualizadas. Por precaución y siguiendo las mejores prácticas, Tenable ha optado por actualizar estos componentes para abordar el posible impacto de los problemas. Security Center 6.6.0 actualiza sqlite a la versión 3.49.1 y ua-parser-js a la versión 0.7.40 para corregir las vulnerabilidades identificadas.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2022-25927 de tipo complejidad ineficiente de expresiones regulares en las versiones del paquete ua-parser-js de 0.7.30 y anteriores a 0.7.33, de 0.8.1 y anteriores a 1.0.33 son vulnerables a la denegación de servicio de expresiones regulares (ReDoS) a través de la función trim().

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-3277 de tipo desbordamiento de búfer basado en montón, podría activar un desbordamiento de entero en la función `concat_ws()` de SQLite. El entero truncado resultante se utiliza para asignar un búfer. Cuando SQLite escribe la cadena resultante en el búfer, utiliza el tamaño original sin truncar, lo que puede provocar un desbordamiento descontrolado del búfer de montón de aproximadamente 4 GB. Esto puede provocar la ejecución de código arbitrario.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-29087 de tipo desbordamiento de entero o envoltura en SQLite 3.44.0 a 3.49.0 (anterior a 3.49.1), la función SQL concat_ws(), puede provocar que se escriba memoria más allá del límite de un búfer asignado por malloc. Si el argumento separador está controlado por el atacante y contiene una cadena grande (p. ej., 2 MB o más), se produce un desbordamiento de entero al calcular el tamaño del búfer de resultados, por lo que malloc podría no asignar suficiente memoria.

A. Productos afectados:

- Tenable Security Center, versión 6.5.1 y anteriores.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión 6.6.0 que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://docs.tenable.com/release-notes/Content/security-center/2025.htm • hxxps://www.tenable.com/security/tns-2025-09 • hxxps://sqlite.org/releaselog/3_49_1.html • hxxps://sqlite.org/src/info/498e3f1cf57f164f • hxxps://github.com/faisalman/ua-parser-js/commit/a6140a17dd0300a35cfc9cff999545f267889411

Índice alfabético