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

114-2025-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°114	Fecha: 16-05-2025 Página: 4 de 11

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Ataque a Coinbase: hackers exigen USD 20 millones para no filtrar información de los usuarios		
Tipo de Ataque	Fuga de Información	Abreviatura	FugaInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K02
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

La industria de las criptomonedas vuelve a ser golpeada por los hackers, en esta ocasión le toca a Coinbase, una plataforma de intercambio de criptomonedas fundada en junio de 2012.

Los ciberdelincuentes han tenido acceso a los datos de los clientes desde enero, incluidos nombres, fechas de nacimiento, direcciones y datos bancarios.

2. DETALLES:

Coinbase ha reconocido un acceso no autorizado a sus sistemas que ha resultado en el robo de datos de los usuarios.

El hackeo ha afectado a usuarios de criptodivisas como Bitcoin, Bitcoin Cash, Ethereum, Litecoin, Dogecoin o Zcash.

Los hackers han realizado un ataque de lo que se conoce como ingeniería social, es decir, utilizan a personas para obtener acceso no autorizado a los datos en lugar de buscar fallos en el código de las plataformas.

Los ciberdelincuentes han sobornado a trabajadores de atención al cliente para obtener acceso a los datos de los usuarios, desde información personal hasta claves bancarias, fecha de creación de las cuentas y su saldo.

“Lo que hacían estos atacantes era encontrar empleados y contratistas de Coinbase con sede en India que estuvieran asociados con nuestras operaciones de subcontratación de procesos comerciales o de soporte, ese tipo de cosas, y sobornarlos para obtener datos de los clientes”, ha explicado el portavoz de la compañía.

Coinbase ha informado que ha recibido un correo electrónico anónimo de los hackers exigiendo el rescate el pasado 11 de mayo, por el que solicitan el pago de 20 millones de dólares para encubrir el robo de información de usuarios de su plataforma de intercambio de criptomonedas.

La plataforma había detectado unos meses atrás que algunos trabajadores de atención al cliente fuera de Estados Unidos recopilaban datos de los sistemas internos, pero no imaginaban la magnitud del problema.

Los datos que obtuvieron incluyen nombre, dirección, teléfono y correo electrónico de los usuarios, pero también los últimos cuatro dígitos de su número de la seguridad Social enmascarado, números de cuentas bancarias enmascarados y algunos identificadores de cuentas bancarias, imágenes de documentos de identificación oficial como carnets de conducir y pasaportes y datos de la cuenta y corporativos.

Según Coinbase, los cibercriminales no lograron acceder a credenciales de inicio de sesión, ni a las claves privadas. Tampoco a capacidades que les permitieran mover fondos entre cuentas. Las cuentas Prime y las billeteras calientes o frías de Coinbase también quedaron fuera del robo de información.

3. RECOMENDACIONES:

- Ejecutar la estrategia 3-2-1-1-0 de copias de seguridad, que consiste en realizar periódicamente tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube; además una de las copias esté disponible fuera de conexión, y cero copias sin verificar o con errores.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados. Estos programas pueden detectar y eliminar ransomware y otro software malicioso antes de que puedan cifrar sus archivos.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones de ransomware
- Habilitar la protección de red para evitar que las aplicaciones o los usuarios accedan a dominios maliciosos y otro contenido malicioso en Internet.
- Habilitar la protección de firewall para monitorear y controlar el tráfico de red entrante y saliente.
- Implementar soluciones de seguridad avanzadas, como sistemas de detección y respuesta de endpoints (EDR), y software de detección y prevención de intrusiones (IDS/IPS), para identificar y bloquear comportamientos sospechosos antes de que causen daños significativos.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.
- En caso de infección, no pagar el rescate ni contactar con los ciberdelincuentes, ya que no hay garantía de que cumplan sus promesas. En su lugar, buscar ayuda profesional para eliminar el ransomware y restaurar los archivos cifrados. Así como también reportar el ransomware a las autoridades.

Fuente de Información:	• hxxps://computerhoy.20minutos.es/ciberseguridad/hackers-van-coinbase-confirma-ciberataque-robo-datos-clientes-1461456 • hxxps://www.infobae.com/estados-unidos/2025/05/15/ataque-a-coinbase-hackers-exigen-usd-20-millones-para-no-filtrar-informacion-de-los-usuarios/ • hxxps://www.escudodigital.com/ciberseguridad/coinbase-renoce-brecha-seguridad-ha-provocado-el-robo-datos-usuarios-intento-chantaje_63399_102.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°114	Fecha: 16-05-2025
		Página: 6 de 11

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

Apple Inc., ha publicado una vulnerabilidad de severidad **MEDIA** de tipo falsificación de solicitud entre sitios (CSRF) que afecta a múltiples sistemas de Apple. La explotación exitosa de esta vulnerabilidad podría permitir el acceso no autorizado a datos a través de sitios web maliciosos.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-31205 de tipo falsificación de solicitud entre sitios, podría permitir que un sitio web malicioso extraiga datos de diferentes orígenes lo que significa que puede acceder indebidamente a información confidencial de diferentes dominios web, lo que supone un riesgo significativo para la privacidad y la seguridad del usuario. La causa principal se debe a comprobaciones insuficientes o incorrectas en los componentes de software afectados.

Actualmente no se conocen exploits públicos ni código de prueba de concepto para esta vulnerabilidad. Además, no se ha reportado ninguna evidencia de explotación activa hasta la fecha.

A. Productos afectados:

- MacOS Sequoia 15.5.
- IOS 18.5.
- IPadOS 18.5.
- WatchOS 11.5.
- TvOS 18.5.
- VisionOS 2.5.
- Safari 18.5.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Implementar políticas estrictas de intercambio de recursos de origen cruzado (CORS) en aplicaciones web.
- Supervisar el tráfico web para detectar patrones inusuales de transferencia de datos.
- Concientizar a los usuarios sobre los riesgos de visitar sitios web no confiables.

Fuente de Información:	• hxxps[:]//support[.]apple[.]com/en-us/122720 • hxxps[:]//support[.]apple[.]com/en-us/122716 • hxxps[:]//support[.]apple[.]com/en-us/122404 • hxxps[:]//support[.]apple[.]com/en-us/122721 • hxxps[:]//support[.]apple[.]com/en-us/122722 • hxxps[:]//support[.]apple[.]com/en-us/122719

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°114	Fecha: 16-05-2025 Página: 7 de 11

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

Arista Networks, Inc., ha publicado una vulnerabilidad de severidad **MEDIA** de tipo almacenamiento de texto simple de una contraseña que afecta a Arista EOS con el transporte gNMI habilitado. La explotación exitosa de esta vulnerabilidad podría permitir que las credenciales del servidor remoto pueden quedar expuestas a través del registro o la contabilidad.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-0936 de tipo almacenamiento de texto simple de una contraseña que afecta a Arista EOS con el transporte gNMI habilitado, podría permitir que las credenciales del servidor remoto pueden quedar expuestas a través del registro o la contabilidad.

En las plataformas afectadas que ejecutan Arista EOS con un transporte gNMI habilitado, ejecutar la RPC gNOI File TransferToRemote con credenciales para un servidor remoto puede provocar que estas credenciales del servidor remoto se registren o contabilicen en el dispositivo EOS local o posiblemente en otros servidores de contabilidad remotos (es decir, TACACS, RADIUS, etc.).

A. Productos afectados:

- Arista EOS, versión 4.30.1F hasta las 4.30.9M en el tren 4.30.x.
- Arista EOS, versión 4.32.3M y anteriores en el tren 4.32.x.
- Arista EOS, versión 4.31.5M y anteriores en el tren 4.31.x.

3. RECOMENDACIÓN:

- Aplicar los parches o mitigaciones proporcionados por Arista para evitar esta exposición de credenciales. La actualización a estas versiones evitará el registro involuntario de credenciales de servidores remotos y reducirá el riesgo de acceso no autorizado.

Fuente de Información:	• hxxps[:]//www[.]arista[.]com/en/support/advisories-notices/security-advisory/21394-security-advisory-0117

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°114	Fecha: 16-05-2025 Página: 8 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en complemento de WP Tabs de 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 **ALTA** de tipo deserialización de datos no confiables que afecta al plugin de WordPress "WP Tabs", desarrollado por ShapedPlugin LLC. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante ejecutar código arbitrario o manipular datos confidenciales en los sitios afectados.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-48134 de tipo deserialización de datos no confiables, podría permitir a un atacante ejecutar código arbitrario o manipular datos confidenciales en los sitios afectados. Esto puede provocar la ejecución de código arbitrario en el sistema afectado, lo que permite a los atacantes manipular o comprometer datos confidenciales del usuario almacenados o procesados por el sitio web mediante el plugin vulnerable.

Actualmente, no se conocen exploits públicos disponibles para esta vulnerabilidad. Hasta el momento no se ha publicado ni observado código de explotación activo

A. Productos afectados:

- WP Tabs para WordPress, todas las versiones hasta 2.2.11.

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/wp-expand-tabs-free/vulnerability/wordpress-wp-tabs-2-2-11-php-object-injection-vulnerability

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°114	Fecha: 16-05-2025
		Página: 9 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en múltiples versiones de PHP		
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 verificación insuficiente de la autenticidad de los datos que afectan a múltiples versiones de PHP. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante enviar URL malformadas que se aceptan incorrectamente como válidas. Esto podría provocar un manejo inadecuado de los datos, su posible modificación o, en algunos casos, una mayor explotación, dependiendo de cómo la aplicación utilice las URLs validadas.

2. DETALLES:

PHP es un lenguaje de programación de código abierto principalmente utilizado para el desarrollo web, que permite crear sitios web dinámicos y aplicaciones.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-5458 de tipo verificación insuficiente de la autenticidad de los datos que afectan a múltiples versiones de PHP, específicamente en la forma en que la función "*filter_var*" valida las URL al usar el filtro "*FILTER_VALIDATE_URL*". Debido a un error lógico, ciertas URL malformadas que contienen información de usuario no válida (nombre de usuario y contraseña) se tratan incorrectamente como válidas, lo que podría permitir que el código posterior acepte y procese estas URL no válidas.

La vulnerabilidad afecta principalmente a la integridad de las aplicaciones, ya que puede permitir a los atacantes enviar URL malformadas que se aceptan incorrectamente como válidas. Esto podría provocar un manejo inadecuado de los datos, su posible modificación o, en algunos casos, una mayor explotación, dependiendo de cómo la aplicación utilice las URL validadas.

A. Productos afectados:

- PHP, versiones anteriores a 7.3.27 – 7.3.33, 7.4.15 – 7.4.33, 8.0.2 – 8.0.30, 8.1.0 – 8.1.28, 8.2.0 – 8.2.19, 8.3.0 – 8.3.7.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la versión PHP 8.1.29, 8.2.20 o 8.3.8 (o posterior) que abordan esta vulnerabilidad.
- Evitar depender exclusivamente de filter_var($url, FILTER_VALIDATE_URL) para casos críticos.
- Añadir comprobaciones manuales de la parte de usuario (username:password@) en URLs, especialmente si contienen caracteres como [o].
- Revisar implementaciones que usen filter_var para validar URLs en flujos sensibles (autenticación, redirecciones, etc).
- Utilizar expresiones regulares personalizadas o bibliotecas especializadas para validar formatos específicos de URLs.
- Restringir el uso de IPv6 en URLs si no es esencial, ya que el error se manifiesta principalmente en URLs con hosts IPv6 que incluyen información de usuario no válida.
- Habilitar logs de errores para detectar intentos de enviar URLs maliciosas y monitorear eventos inusuales en aplicaciones.

Fuente de Información:	• hxxp://www.openwall.com/lists/oss-security/2024/06/07/1 • hxxps://github.com/php/php-src/security/advisories/GHSA-w8qr-v226-r27w • hxxps://lists.debian.org/debian-lts-announce/2024/06/msg00009.html • hxxps://security.netapp.com/advisory/ntap-20240726-0001/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°114	Fecha: 16-05-2025 Página: 10 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades en ThinServer de Rockwell Automation ThinManager		
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 permisos predeterminados incorrectos y restricción inadecuada de operaciones dentro de los límites de un búfer de memoria que afecta al software ThinManager de Rockwell Automation. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante local obtener privilegios elevados y provocar una denegación de servicio (DoS) en el software objetivo.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-3617 de tipo permisos predeterminados incorrectos en ThinManager de Rockwell Automation, podría permitir a un atacante local heredar privilegios elevados. Existe una vulnerabilidad de escalada de privilegios en el producto afectado. Al iniciarse el software, se eliminan archivos de la carpeta temporal, lo que provoca que la entrada de control de acceso del directorio herede los permisos del directorio principal. Si se explota, un atacante podría heredar privilegios elevados.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-3618 de tipo restricción inadecuada de operaciones dentro de los límites de un búfer de memoria en ThinManager, podría permitir a un atacante provocar una denegación de servicio en el software objetivo. El software no verifica adecuadamente el resultado de la asignación de memoria al procesar mensajes de tipo 18.

A. Productos afectados:

- ThinManager, versión 14.0.1 y anteriores.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión 14.0.2 o posterior que aborda estas vulnerabilidades.
- Limitar el acceso de usuarios locales a los sistemas ThinManager.
- Implementar controles de acceso estrictos y monitorear los cambios de permisos.
- Actualizar periódicamente las políticas de control de acceso.
- Aislar los sistemas afectados si no es posible aplicar parches de inmediato.
- Minimizar la exposición de la red.
- Colocar los sistemas de control detrás de firewalls y separados de las redes comerciales.
- Utilizar métodos de acceso remoto seguros, como VPN, y manténgalos actualizados.

Fuente de Información:	• hxxps://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1727.html

Índice alfabético