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

087-2025-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°087	Fecha: 11-04-2025
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El ladrón TROX recopila datos confidenciales, incluidas tarjetas de crédito almacenadas y credenciales del navegador		
Tipo de Ataque	Stealers	Abreviatura	Stealers
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C03
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES:**

Los expertos en ciberseguridad de Sublime han descubierto una compleja campaña de malware que gira en torno a TROX Stealer, un ladrón de información, detectado por primera vez en diciembre de 2024, que utiliza la urgencia para engañar a las víctimas.

2. **DETALLES:**

Este malware destaca por una intrincada cadena de ataque diseñada para extraer datos confidenciales de los consumidores comunes.

El éxito de TROX Stealer depende de la táctica psicológica de la urgencia, que impulsa a las víctimas a pasar por alto el pensamiento crítico.

Los atacantes utilizan correos electrónicos que parecen urgentes y tienen asuntos como “Última oportunidad para liquidar una deuda antes de una acción legal” o “Advertencia final: acción legal pendiente para su cuenta”, lo que crea una sensación de pánico.

Los correos contenían texto generado en HTML con un enlace para descargar supuestos documentos legales.

Este enlace redirigía a un dominio controlado por el atacante, donde estaba alojado el malware, disfrazado como 'DebtCollectionCase#######.exe'.

La URL incluía un ID de token, lo que garantizaba que la descarga solo se produjera una vez, evitando así que los investigadores volvieran a descargar fácilmente el archivo para su análisis.

El proceso de instalación de TROX Stealer se caracteriza por varias técnicas de evasión:

Entrega inicial: un script de Python compilado por Nuitka , envuelto en múltiples capas de ofuscación, se descarga como un ejecutable de Windows desde el dominio del atacante.

Ejecución: El archivo descargado descomprime los archivos incrustados en una carpeta temporal, ejecutando 'client_pdf_case_388.pdf', un documento señuelo, y 'node700.exe', un intérprete de Node.JS, y además ejecuta scripts para mantener la infección.

WebAssembly: el malware utiliza código WebAssembly (Wasm) codificado en Base64, empleando código basura extenso para ocultar su funcionalidad y dificultar el análisis.

La infraestructura detrás de TROX Stealer incluye varios dominios y direcciones IP, con una gestión de certificados rutinaria que garantiza su persistencia.

Las plataformas de malware como servicio (MaaS) facilitan la rápida implementación y la iteración de campañas de ataque a gran escala por parte de los atacantes.

INDICADORES DE COMPROMISO:

Categoría	Identificador	Valor
Dominio	debt-collection-experts[.]com	

Dominio	documents[.]debt-collection-experts[.]com	
Dominio	debt-collection-experts[.]online	
Dominio	download.debt-collection-experts[.]online	
Dominio	downloads.debt-collection-experts[.]online	
Dominio	docs.debt-collection-experts[.]online	
Dirección IP	89.185.82.34 – Central to this campaign's operations	89.185.82.34
Dirección IP	172.22.117.177 – Recibe perfiles del sistema del malware	172.22.117.177
Archivo hash	DebtCollectionCase#######.exe (SHA256)	c404baad60fa3e6bb54a38ab2d736238ccaa06af877da6794e0e4387f8f5f0c6
Archivo hash	DebtCollectionCase#######.exe (SHA1)	ae5166a8e17771d438d2d5e6496bee948fce80a4
Archivo hash	DebtCollectionCase#######.exe (MD5)	c568b578da49cfcdb37d1e15a358b34a
Archivo hash	node700.exe (SHA256)	12069e203234812b15803648160cc6ad1a56ec0e9cebaf12bad249f05dc782ef
Archivo hash	node700.exe (SHA1)	29a13e190b6dd63e227a7e1561de8edbdeba034b
Archivo hash	node700.exe (MD5)	f5f75c9d71a891cd48b1ae9c7cc9f80d
Archivo hash	TROX Stealer (SHA256)	5d7ed7b8300c94e44488fb21302a348c7893bdaeef80d36b78b0e7f0f20135df
Archivo hash	TROX Stealer (SHA1)	6deea67690f90455280bc7dfed3c69d262bf24f6
Archivo hash	TROX Stealer (MD5)	fedb7287bcccc256a8dad8aeace799f7
Correo	vpn@esystematics[.]de	
Correo	vpn@contactcorporate[.]de	
Correo	vpn@evirtual-provider[.]de	

3. RECOMENDACIONES:

- Adaptar medidas de ciberseguridad, integrando IA y análisis avanzados para anticiparse a estas complejas amenazas.
- 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.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://gbhackers.com/trox-stealer-harvests-sensitive-data-including-stored-credit-cards/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°087	Fecha: 11-04-2025 Página: 6 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el plugin InstaWP Connect 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:

Wordfence ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo recorrido de ruta en el plugin InstaWP Connect para WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar archivos arbitrarios en el servidor afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-2636 de tipo recorrido de ruta de inclusión de archivos locales en el plugin InstaWP Connect para WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado incluir y ejecutar archivos arbitrarios en el servidor afectado.

Los atacantes pueden ejecutar código PHP arbitrario incluyendo archivos en el servidor. Esto puede llevar a eludir controles de acceso, exponer datos confidenciales o lograr la ejecución de código no autorizado.

La vulnerabilidad existe en el parámetro *'instawp-database-manager'*, lo que permite a un atacante no autenticado incluir y ejecutar archivos arbitrarios en el servidor. Un atacante remoto no autenticado podría evitar los controles de acceso, ejecutar código PHP arbitrario, obtener datos confidenciales y lograr un compromiso total del sistema.

A. Productos afectados:

- Plugin InstaWP Connect para WordPress, todas las versiones hasta la 0.1.0.85 (inclusive).

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Deshabilitar temporalmente el complemento en caso no sea posible actualizar el plugin.
- Eliminar el complemento de las instalaciones de WordPress.
- Implementar reglas de firewall de aplicaciones web (WAF) para bloquear la explotación potencial.
- Monitorear los registros del servidor para detectar intentos sospechosos de inclusión de archivos.

Fuente de Información:	• hxxps://plugins.trac.wordpress.org/browser/instawp-connect/trunk/includes/database-manager/loader.php#L77 • hxxps://plugins.trac.wordpress.org/changeset/3269681/ • hxxps://www.wordfence.com/threat-intel/vulnerabilities/id/4c8f2c6f-c231-477c-895b-df892569ef95?source=cve

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°087	Fecha: 11-04-2025 Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Ivanti Connect Secure		
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:

Ivanti ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo desbordamiento de búfer basado en pila en Ivanti Connect Secure. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto autenticado ejecutar código arbitrario en el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-22467 de tipo desbordamiento de búfer basado en pila en Ivanti Connect Secure, podría permitir a un atacante remoto autenticado ejecutar código arbitrario en el sistema afectado.

Esta vulnerabilidad permite la ejecución remota de código con baja complejidad y requisitos de privilegios reducidos. Un atacante autenticado podría comprometer la confidencialidad del sistema, modificar o eliminar datos críticos del sistema y tomar el control total del dispositivo afectado.

Se identificaron aproximadamente 2,850 casos como vulnerables a nivel mundial, con las concentraciones más altas en los EE. UU. (852 casos) y Japón (384 casos). La vulnerabilidad requiere acceso autenticado, lo que limita su explotabilidad en comparación con las vulnerabilidades no autenticadas.

Ivanti indicó que a la fecha no se conocen exploits para esta vulnerabilidad que se estén utilizando de forma activa. Asimismo, Ivanti declaró en el momento de la divulgación de la vulnerabilidad (febrero de 2025) que no había observado ninguna evidencia de explotación. Además, no existe ninguna prueba de concepto (PoC) pública disponible para esta vulnerabilidad.

A. Productos afectados:

- Ivanti Connect Secure, versiones anteriores a 22.7R2.6.

3. RECOMENDACIONES:

- Actualizar Ivanti Connect Secure a la versión 22.7R2.6 o posterior.
- Implementar una segmentación estricta de la red.
- Limitar y monitorear el acceso administrativo.
- Habilitar el registro y la monitorización mejorados para posibles intentos de explotación.
- Realizar una evaluación de seguridad exhaustiva del entorno.
- Verificar que no haya indicios de compromiso previo.

Fuente de Información:	• hxxps://forums.ivanti.com/s/article/February-Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-and-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°087	Fecha: 11-04-2025
		Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en la herramienta Langflow		
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:

VulnCheck ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo falta autenticación faltante para función crítica en la herramienta Langflow. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en servidores Langflow sin necesidad de autenticación, lo que supone un grave riesgo para la seguridad de estos sistemas.

2. DETALLES:

Langflow es un potente generador de IA de bajo código, diseñado para crear e implementar agentes y flujos de trabajo basados en IA, especialmente en aplicaciones de generación aumentada por recuperación (RAG) y multiagente.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-3248 de tipo autenticación faltante para función crítica en la herramienta Langflow. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado enviar solicitudes HTTP manipuladas para ejecutar código arbitrario y comprometer el sistema. Esto puede tener graves consecuencias, como fugas de datos, interrupciones del sistema y otras actividades maliciosas.

El problema principal reside en un endpoint de API no autenticado (/api/v1/validate/code) que ejecuta la función exec de Python al recibir una entrada de usuario no confiable. Si bien Langflow permite a los usuarios autenticados modificar y ejecutar código Python, esta vulnerabilidad abre la puerta a atacantes no autenticados. Los atacantes pueden inyectar código malicioso, como una shell inversa de Python, en un decorador o en el argumento predeterminado de una función para lograr la ejecución remota de código.

VulnCheck indicó que existen exploits conocidos para esta vulnerabilidad, que permite a los atacantes ejecutar código arbitrario en servidores Langflow sin autenticación.

A. Productos afectados:

- Langflow, versiones anteriores a la 1.3.0.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://github.com/langflow-ai/langflow/pull/6911 • hxxps://github.com/langflow-ai/langflow/releases/tag/1.3.0 • hxxps://www.horizon3.ai/attack-research/disclosures/unsafe-at-any-speed-abusing-python-exec-for-unauth-rce-in-langflow-ai/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°087	Fecha: 11-04-2025
		Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Google Chrome para Windows		
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 **CRÍTICA** de tipo error de validación de entrada en Mojo en Google Chrome para Windows. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir la protección sandbox de Chrome, lo que les permite ejecutar código malicioso en el sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica de día cero** identificada por MITRE como CVE-2025-2783 de tipo error de validación de entrada en Google Chromium, podría permitir a un atacante remoto no autenticado eludir la protección sandbox de Chrome, lo que les permite ejecutar código malicioso en el sistema.

La vulnerabilidad implica un "controlador incorrecto proporcionado en circunstancias no especificadas en Mojo en Windows", donde Mojo es el marco de comunicación entre procesos de Chromium. La vulnerabilidad se debe a una validación insuficiente de la información proporcionada por el usuario, relacionada con Mojo en Windows. Un atacante remoto puede engañar a la víctima para que visite un sitio web especialmente diseñado y ejecute código arbitrario en el sistema.

La vulnerabilidad se explotó junto con otro exploit para la ejecución remota de código. Los ataques consistieron en correos electrónicos de phishing con enlaces a sitios web comprometidos, que activaban los exploits al abrirse en Chrome

Cabe indicar que esta vulnerabilidad se utilizó en una sofisticada campaña de ciberespionaje conocida como "Operación ForumTroll", dirigida a organizaciones rusas mediante correos electrónicos de phishing.

A. Productos afectados:

- Google Chromium: versiones anteriores a 134.0.6998.177/178.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Evitar hacer clic en enlaces sospechosos o abrir archivos adjuntos de fuentes.
- Activar la Navegación segura mejorada en la configuración de Chrome para mejorar la protección contra sitios web y descargas maliciosas.
- Utilizar software de protección de puntos finales para supervisar y bloquear actividades maliciosas en su sistema.
- Revisar periódicamente la configuración de seguridad de su sistema y asegúrese de que todo el software esté actualizado para evitar la explotación de vulnerabilidades similares.

Fuente de Información:	• hxxps://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html • hxxps://crbug.com/405143032

Índice alfabético