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

119-2025-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°119	Fecha: 22-05-2025
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Microsoft desmantela la red de robo de datos Lumma y confisca más de 2.000 dominios		
Tipo de Ataque	Stealers	Abreviatura	Stealers
Medios de propagación	USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	C	Código de Sub familia	C03
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

El Centro Europeo de Ciberdelincuencia de Europol ha colaborado con Microsoft para desmantelar Lumma Stealer, la amenaza de robo de información más importante del mundo, conocida por ser responsable del robo generalizado de credenciales, fraude financiero y ataques de ransomware.

2. DETALLES:

Lumma Stealer se ha comercializado en foros clandestinos desde al menos 2022 como una solución lista para usar para ciberdelincuentes que buscan robar todo, desde contraseñas y números de tarjetas de crédito hasta monederos de criptomonedas y credenciales bancarias. La herramienta se suele propagar mediante campañas de phishing, malvertising y cargadores de malware.

La plataforma Lumma funcionaba como un centro de compraventa de malware, proporcionando a los delincuentes un acceso fácil a funciones avanzadas de robo de datos. Su amplio uso y accesibilidad lo convirtieron en la opción preferida de los ciberdelincuentes que buscaban explotar datos personales y financieros.

El equipo de Inteligencia de Amenazas de Microsoft ha seguido de cerca las actividades de Lumma, identificando patrones de infección generalizados entre marzo y mayo de 2025. Los mapas de calor compartidos por la compañía ilustran la huella global de este malware, con altas concentraciones de dispositivos infectados en América del Norte, Europa y partes de Asia.

Europol actuó como punto central en Europa para el intercambio y la coordinación de inteligencia. Tras recibir información crítica de Microsoft, el Centro Europeo de Ciberdelincuencia de Europol enriqueció esta información y proporcionó a los Estados miembros una visión del panorama de amenazas para garantizar una comprensión clara de las operaciones de la red.

En una acción coordinada, el Departamento de Justicia de los Estados Unidos (DOJ) confiscó el panel de control de Lumma, crucial para el mercado de Lumma. La colaboración de Microsoft con el Centro de Control de Ciberdelincuencia de Japón (JC3) también condujo a la suspensión de la infraestructura de Lumma con sede en Japón.

3. RECOMENDACIONES:

- Coordinar con entidades nacionales e internacionales el uso de espacios colaborativos para generar una respuesta rápida a la eliminación de ciberdelitos a nivel global.
- Establecer mecanismos de intercambio de inteligencia de amenazas con el objetivo de generar sistemas defensivos más fuertes y encontrar otras estrategias.
- No abrir enlaces ni descargar archivos sospechosos, ni responder a correos electrónicos no confiables ni mensajes de texto.
- Utilizar herramientas antivirus y antimalware confiables oficiales.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones, actualizados con los últimos parches y actualizaciones de seguridad.
- Habilitar la autenticación multifactor (MFA) en todas las plataformas que sea posible.
- Educar a los usuarios sobre cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2025/05/desmantelando-lumma-stealer.html • hxxps://hackread.com/microsoft-dismantle-lumma-stealer-domain-seized/ • hxxps://www.infobae.com/america/agencias/2025/05/22/microsoft-desarticula-la-principal-infraestructura-del-malware-de-robo-de-informacion-internacional-lumma-stealer/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°119	Fecha: 22-05-2025 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en Adobe Dreamweaver V8		
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:

Adobe Systems Incorporated ha publicado una vulnerabilidad de severidad **ALTA** de tipo confusión de tipos que afecta a Adobe Dreamweaver Desktop. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el contexto del usuario actual.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-30310 de tipo confusión de tipos que afecta Adobe Dreamweaver Desktop, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el contexto del usuario actual. Para explotarla, se requiere la interacción del usuario, ya que el objetivo debe visitar una página maliciosa o abrir un archivo malicioso.

La vulnerabilidad existe en el motor JavaScript de Dreamweaver, específicamente debido al uso de una versión vulnerable del motor V8. Un atacante puede explotar este problema convenciendo al usuario de abrir un archivo especialmente diseñado o visitar una página web maliciosa. Una explotación exitosa permite la ejecución de código arbitrario en el contexto del usuario actual, lo que podría comprometer por completo el sistema si el usuario tiene permisos de administrador.

A la fecha, no existe un exploit conocido públicamente ni código de prueba de concepto para la explotación de esta vulnerabilidad.

A. Productos afectados:

- Adobe Dreamweaver Desktop, versión 21.4 y anteriores para plataforma Windows y macOS.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad. En entornos administrados, los administradores de TI pueden usar Creative Cloud Packager para la implementación.
- Aplicar el principio de mínimo privilegio para las cuentas de usuario.
- Restringir los privilegios de administrador a cuentas dedicadas.
- Habilitar funciones antiexplotación cuando sea posible.

Fuente de Información:	• hxxps://www.zerodayinitiative.com/advisories/ZDI-25-308/ • hxxps://helpx.adobe.com/security/products/dreamweaver/apsb25-35.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°119	Fecha: 22-05-2025
		Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en productos Cisco		
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 múltiples vulnerabilidades de severidad **ALTA** de tipo lectura fuera de límites, aplicación de la seguridad del lado del servidor en el lado del cliente y omisión de autorización mediante clave controlada por el usuario que afecta a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado escalar privilegios y provocar una condición de denegación de servicio (DoS) en el dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-20152 de tipo lectura fuera de límites en la función de procesamiento de mensajes RADIUS de Cisco Identity Services Engine (ISE), podría permitir que un atacante remoto no autenticado provoque una condición de DoS en un dispositivo afectado. Esta vulnerabilidad se debe a la gestión incorrecta de ciertas solicitudes RADIUS. Un atacante podría explotarla enviando una solicitud de autenticación específica a un dispositivo de acceso a la red (NAD) que utiliza Cisco ISE para autenticación, autorización y contabilidad (AAA). Una explotación exitosa podría permitir al atacante provocar la recarga de Cisco ISE.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-20113 de tipo aplicación de la seguridad del lado del servidor en el lado del cliente en Cisco Unified Intelligence Center, podría permitir que un atacante remoto autenticado eleve privilegios a Administrador para un conjunto limitado de funciones en un sistema afectado. Esta vulnerabilidad se debe a una validación insuficiente del lado del servidor de los parámetros proporcionados por el usuario en las solicitudes API o HTTP. Un atacante podría explotar esta vulnerabilidad enviando una solicitud API o HTTP manipulada a un sistema afectado. Una explotación exitosa podría permitir al atacante acceder, modificar o eliminar datos fuera del alcance de su nivel de acceso previsto, incluyendo la obtención de información confidencial almacenada en el sistema.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-20114 de tipo omisión de autorización mediante clave controlada por el usuario en la API de Cisco Unified Intelligence Center, podría permitir que un atacante remoto autenticado realice un ataque de escalada de privilegios horizontal en un sistema afectado. Esta vulnerabilidad se debe a una validación insuficiente de los parámetros proporcionados por el usuario en las solicitudes de API. Un atacante podría explotar esta vulnerabilidad enviando solicitudes de API manipuladas a un sistema afectado para ejecutar un ataque de referencia directa a objetos inseguro.

A. Productos afectados:

- La vulnerabilidad CVE-2025-20152 afecta a Cisco ISE versión 3.3 y anteriores, si está configurado con servicios de autenticación RADIUS. Si Cisco ISE se utiliza únicamente para TACACS+, el dispositivo de red no se verá afectado por esta vulnerabilidad.
- Las vulnerabilidades CVE-2025-20113 y CVE-2025-20114 afectan a Cisco Unified Intelligence Center, independientemente de la configuración del dispositivo, incluso si se utiliza como parte de las siguientes soluciones de Cisco: Centro de contacto empresarial empaquetado (CCE empaquetado) y Centro de contacto unificado empresarial (Unified CCE). Estas vulnerabilidades también afectan a Cisco Unified Contact Center Express (Unified CCX) porque Cisco Unified CCX incluye Cisco Unified Intelligence Center como parte de su paquete de software.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-restart-ss-uf986G2Q • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuis-priv-esc-3Pk96SU4

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°119	Fecha: 22-05-2025 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de desbordamiento de búfer en macOS		
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 **ALTA** de tipo desbordamiento de búfer en macOS. La explotación exitosa de esta vulnerabilidad 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-2025-31233 de tipo desbordamiento de búfer en macOS, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad existe debido a un error de límite en CoreMedia al procesar archivos de vídeo. Un atacante remoto puede crear un archivo de vídeo especialmente diseñado, engañar a la víctima para que lo abra, provocar corrupción de memoria y ejecutar código arbitrario en el sistema objetivo. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

A. Productos afectados:

- macOS: 15.0 24A335, 15.0.1 24A348, 15.1 24B83, 15.1.1 24B91, 15.1.1 24B2091, 15.2 24C101, 15.3 24D60, 15.3.1 24D70, 15.3.2 24D81, 15.3.2 24D2082, 15.4 24E248, 15.4.1 24E263.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la versión 15.5 que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://support.apple.com/en-us/122716 • hxxps://www.zerodayinitiative.com/advisories/ZDI-25-298/

Índice alfabético