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

085-2025-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°085	Fecha: 09-04-2025
		Página: 4 de 11

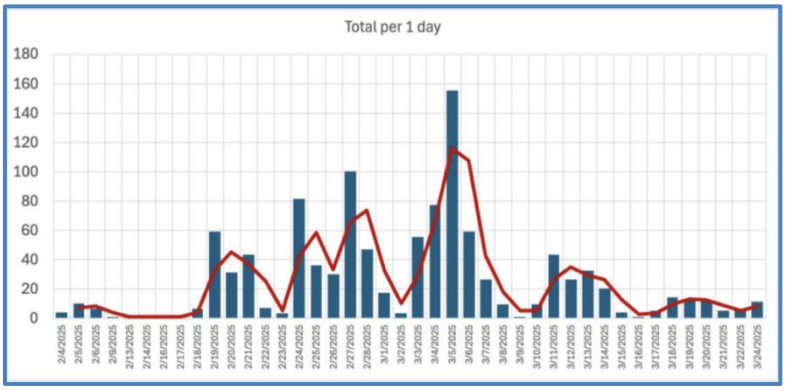
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Grandoreiro ataca de nuevo: ataques de phishing geocercados en Latinoamérica		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Una nueva campaña de phishing se dirige a usuarios de toda Latinoamérica, centrada en Grandoreiro, un troyano bancario conocido por robar datos financieros confidenciales.

Entre el 19 de febrero y el 14 de marzo, los investigadores notaron un aumento en la actividad de phishing vinculada a Grandoreiro, y hay señales que muestran que la campaña aún está en curso.



2. DETALLES:

Una de las técnicas más destacadas de esta campaña es el geofencing. Antes de ejecutarse, el malware verifica la dirección IP de la víctima para determinar su ubicación, centrándose en ubicaciones de latinoamérica, para así optimizar el enfoque de la campaña, reducir la exposición innecesaria y eludir la vigilancia de seguridad global.
La infección comienza con una página de phishing que induce a la víctima a hacer clic en un enlace o descargar un documento PDF falso. En lugar de un PDF, el archivo es en realidad un archivo comprimido (.ZIP o .RAR) que contiene el cargador Grandoreiro.
Una vez extraído y abierto el archivo, el malware envía una solicitud a ip-apicom para determinar la geolocalización del usuario, si coincide con una región objetivo, el ataque continúa.
Grandoreiro evita las consultas DNS locales enviando una solicitud a [nombre del dominio dns.google]. Proporciona el nombre de dominio de su servidor de comando y control (C2), que Google resuelve a una dirección IP.
Este paso le ayuda a eludir los mecanismos de bloqueo basados en DNS y mejora sus posibilidades de comunicación exitosa.
Tras resolver el dominio C2, el malware envía una solicitud GET a la dirección IP obtenida para establecer una conexión.
Tras establecer una conexión con el servidor C2, el atacante puede permanecer oculto, enviar cargas útiles adicionales, robar credenciales y recopilar datos, tomar el control remoto del equipo infectado, y prepararse para una mayor explotación.

3. RECOMENDACIONES:

- Permanecer atento a los engaños de phishing que se hacen pasar por descargas de PDF (a menudo, archivos .ZIP o .RAR).
- Supervisar las solicitudes de DNS externas, especialmente a dns.google, justo después de la ejecución.
- Marcar las búsquedas de geolocalización en servicios como ip-apicom; es una parte clave de la táctica de filtrado de Grandoreiro.
- Utilizar el análisis basado en el comportamiento para detectar tácticas posteriores a la ejecución, como la eliminación de archivos, el acceso a credenciales o el descubrimiento del sistema.
- Tomar conciencia y capacitarse para identificar correos maliciosos.

Fuente de Información:	• hxxps://hackread.com/grandoreiro-strikes-geofenced-phishing-attacks-latam/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°085	Fecha: 09-04-2025
		Página: 5 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el controlador del kernel del Sistema de Archivos de Registro Común de 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:

Microsoft Corporation ha lanzado una actualización de seguridad que corrige una vulnerabilidad **CRÍTICA** de día cero de tipo uso después de la liberación en el controlador del kernel del Sistema de Archivos de Registro Común de Windows (CLFS). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante local autorizado elevar privilegios de SYSTEM en equipos Windows comprometidos.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-29824 de tipo uso después de la liberación en el controlador del kernel del Sistema de Archivos de Registro Común de Windows (clfs.sys), podría permitir a un atacante local autorizado obtener privilegios de SYSTEM en equipos Windows comprometidos.

La vulnerabilidad surge cuando el controlador CLFS hace referencia a memoria ya liberada, lo que provoca corrupción de memoria. Su explotación implica sobrescribir tokens de proceso mediante la RtlSetAllBitsAPI, lo que permite a los atacantes inyectar procesos en operaciones a nivel de SYSTEM.

Un atacante con privilegios de bajo nivel puede escalar a privilegios de SYSTEM, lo que podría permitirle obtener el control total del sistema Windows afectado. Esto podría provocar modificaciones no autorizadas del sistema, robo de datos, instalación de malware o creación de nuevas cuentas de usuario con plenos derechos administrativos.

La vulnerabilidad se está explotando activamente en la naturaleza. Esta vulnerabilidad se ha vinculado a campañas de ransomware organizadas por actores de amenaza identificados como Storm-2460. Los atacantes utilizan un troyano llamado PipeMagic para distribuir el exploit y desplegar cargas útiles de ransomware. Los objetivos de estos ataques han incluido organizaciones de los sectores de TI, bienes raíces, finanzas y venta minorista en países como Estados Unidos, Venezuela, España y Arabia Saudita.

A. Productos afectados:

- Múltiples versiones de Windows 10 (sistemas x64 y de 32 bits), Windows 11, Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, 2022, 2025.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad. La actualización de seguridad para Windows 10 para sistemas x64 y Windows 10 para sistemas de 32 bits no está disponible de inmediato. Las actualizaciones se publicarán lo antes posible y, cuando estén disponibles, se notificará a los clientes mediante una revisión de esta información de CVE.
- Utilizar herramientas EDR/XDR para detectar comportamientos anómalos relacionados con clfs.sys.
- Limitar el acceso a sistemas vulnerables y aplicar principios de mínimo privilegio.
- Priorizar la aplicación de parches para todas las versiones de Windows afectadas.
- Supervisar los sistemas para detectar intentos sospechosos de escalada de privilegios.
- Considerar la protección y el monitoreo adicionales de los puntos finales.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-29824?utm_source=feedly

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°085	Fecha: 09-04-2025 Página: 6 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el paquete de base de datos de Joomla Framework		
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:

Joomla Project ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo inyección SQL en el método quoteNameStr del paquete de base de datos del framework Joomla. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar comandos SQL no autorizados, acceder, modificar o eliminar información confidencial de la base de datos del framework Joomla.

2. DETALLES:

Joomla es un sistema de gestión de contenidos (CMS) gratuito y de código abierto que permite a los usuarios construir y gestionar sitios web sin necesidad de tener conocimientos profundos de programación.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-25226 de tipo inyección SQL en el método quoteNameStr del paquete de base de datos del framework Joomla. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar comandos SQL no autorizados, acceder, modificar o eliminar información confidencial de la base de datos del framework Joomla.

La vulnerabilidad existe en un método protegido sin usos directos en los paquetes originales (ramas 2.x y 3.x). Sin embargo, las clases personalizadas que extienden la clase de base de datos afectada podrían ser vulnerables si utilizan dicho método.

Un atacante podría explotar esta vulnerabilidad para ejecutar comandos SQL no autorizados, comprometer la integridad de la base de datos: acceder, modificar o eliminar información confidencial de la base de datos, evitar la autenticación o los controles de acceso. La vulnerabilidad puede explotarse remotamente sin interacción del usuario.

Actualmente no se conocen exploits ni malware que exploten esta vulnerabilidad.

A. Productos afectados:

- Paquete de base de datos Joomla, versión 1.0 a 3.3.1.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Revisar y auditar las clases de base de datos personalizadas que extienden la clase base.
- Implementar la validación de entrada y las consultas parametrizadas.
- Limitar los privilegios de usuario de la base de datos.
- Monitorear actividades sospechosas de consultas de bases de datos.

Fuente de Información:	• hxxps://developer.joomla.org/security-centre/963-20250401-framework-sql-injection-vulnerability-in-quotenamestr-method-of-database-package.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°085	Fecha: 09-04-2025
		Página: 7 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el administrador de Datos SENTRON 7KT PAC1260		
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:

Siemens AG ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo uso de credenciales codificadas en el administrador de Datos SENTRON 7KT PAC1260 de Siemens. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener acceso root al sistema operativo del dispositivo, especialmente si el servicio SSH está habilitado.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-41794 de tipo uso de credenciales codificadas en el administrador de Datos SENTRON 7KT PAC1260, podría permitir a un atacante remoto no autenticado obtener acceso root al sistema operativo del dispositivo, especialmente si el servicio SSH está habilitado. Un atacante con acceso a la red podría obtener privilegios completos de nivel raíz en el dispositivo, acceder y manipular sistemas de infraestructura críticos y ejecutar comandos arbitrarios con privilegios máximos del sistema.

Esta vulnerabilidad se debe a la presencia de credenciales codificadas que permiten el acceso remoto al sistema operativo del dispositivo con privilegios de root. Si el servicio SSH está habilitado, un atacante remoto no autenticado podría explotar estas credenciales para obtener el control total del dispositivo.

Actualmente, no existe evidencia de una prueba de concepto (PoC) pública ni de exploits conocidos para CVE-2024-41794.

A. Productos afectados:

- SENTRON 7KT PAC1260 Data Manager (todas las versiones).

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Deshabilitar servicios innecesarios, como SSH, en los dispositivos afectados para reducir los vectores de ataque.
- Implementar la segmentación de red para aislar estos dispositivos.
- Usar controles de acceso a la red adicionales.
- Monitorear los intentos de acceso no autorizado.
- Realizar una evaluación de seguridad exhaustiva de todos los dispositivos SENTRON 7KT PAC1260 Data Manager.

Fuente de Información:	• hxxps://securityonline.info/siemens-security-alert-critical-vulnerabilities-in-sentron-7kt-pac1260-data-manager/ • hxxps://cert-portal.siemens.com/productcert/html/ssa-187636.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°085	Fecha: 09-04-2025 Página: 8 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Microsoft SharePoint Server		
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 una vulnerabilidad de severidad **ALTA** de tipo autorización indebida que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante autenticado la ejecución remota de código en el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-29794 de tipo ejecución remota de código (RCE), podría permitir a un atacante autenticado con permisos de propietario de sitio podría inyectar y ejecutar código arbitrario de forma remota en SharePoint Server. Cualquier atacante autenticado podría activar esta vulnerabilidad. No requiere privilegios de administrador ni otros privilegios elevados.

En un ataque basado en red, un atacante autenticado, como al menos el propietario del sitio, podría escribir código arbitrario para inyectar y ejecutar código de forma remota en el servidor SharePoint.

A. Productos afectados:

- Microsoft SharePoint Server Subscription Edition versión 16.0.0 hasta la 16.0.18526.20172.
- Microsoft SharePoint Server 2019 versión 16.0.0 antes de 16.0.10417.20003.
- Microsoft SharePoint Enterprise Server 2016 versión 16.0.0 antes de 16.0.5495.1002.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//msrc[.]Microsoft[.]com/update-guide/vulnerability/CVE-2025-29794

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°085	Fecha: 09-04-2025 Página: 9 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Adobe Photoshop para Windows y 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:

Adobe Systems Incorporated ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo desbordamiento de búfer basado en montón que afecta Adobe Photoshop. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en el contexto del usuario actual, siempre que este interactúe con un archivo malicioso, como abrirlo.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-27198 de tipo desbordamiento de búfer basado en montón que afecta Adobe Photoshop Desktop, podría permitir a un atacante autenticado con permisos de propietario de sitio inyectar y ejecutar código arbitrario de forma remota en SharePoint Server.

A. Productos afectados:

- Adobe Photoshop 2025, 26.4.1 y versiones anteriores en las plataformas de Windows y macOS.
- Adobe Photoshop 2024, 25.12.1 y versiones anteriores en las plataformas de Windows y macOS.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- No abrir archivos de fuentes desconocidas. Dado que la explotación requiere la interacción del usuario (abrir un archivo malicioso), evitar archivos sospechosos puede reducir significativamente el riesgo.
- Mantenga todo el software actualizado, ya que las versiones más nuevas suelen incluir parches de seguridad.
- Utilizar software antivirus para escanear los archivos antes de abrirlos.
- Educar a los usuarios sobre los riesgos asociados con la apertura de archivos de fuentes no confiables.

Fuente de Información:	• hxxps[:]//helpx[.]adobe[.]com/security/products/photoshop/apsb25-30.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°085	Fecha: 09-04-2025
		Página: 10 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en CentreStack de Gladinet		
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:

Gladinet, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo uso de clave criptográfica codificada en CentreStack. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema con privilegios de la cuenta del servidor web Microsoft IIS.

2. DETALLES:

Gladinet CentreStack es una robusta solución empresarial diseñada para el intercambio seguro de archivos, el acceso móvil y la integración en la nube híbrida. Se integra con la infraestructura de TI existente y ofrece funciones como protección contra ransomware, integración con Active Directory y almacenamiento en la nube escalable.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-30406 de tipo uso de clave criptográfica codificada en Gladinet CentreStack de Microsoft, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema con privilegios de la cuenta del servidor web Microsoft IIS. La explotación exitosa de la vulnerabilidad puede permitir a un atacante ejecutar código arbitrario en el sistema con privilegios de la cuenta del servidor web Microsoft IIS.

La vulnerabilidad se debe al uso de una clave criptográfica codificada de forma rígida al cifrar datos de ViewState. Un atacante remoto no autenticado puede predecir la clave de máquina en uso y falsificar cargas útiles de ViewState que superen las comprobaciones de integridad. Tener en cuenta que esta vulnerabilidad está siendo explotada activamente en la naturaleza.

A. Productos afectados:

- CentreStack: 12.4.9458.51242 - 16.1.10296.56315.

3. RECOMENDACIONES:

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

Fuente de Información:	• hxxps://gladinetsupport.s3.us-east-1.amazonaws.com/gladinet/securityadvisory-cve-2005.pdf • hxxps://www.centrestack.com/p/gce_latest_release.html

Índice alfabético