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

099-2025-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°099	Fecha: 28-04-2025
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El kit de phishing Darcula utiliza inteligencia artificial para evadir la detección		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

El 23 de abril, Netcraft detectó la integración de IA generativa en Darcula-Suite, lo que permite a los usuarios generar formularios de phishing en cualquier idioma, personalizar campos de formulario y traducir automáticamente formularios completos manteniendo el diseño original.

2. DETALLES:

Darcula es un modelo de servicio diseñado para su expansión. Ofrece a los usuarios herramientas para imitar organizaciones en diversos países, desarrolladas con tecnologías modernas como frameworks JavaScript, Docker y Harbor, replicando la configuración de empresas SaaS (software como servicio) legítimas. Los operadores utilizan SMS, RCS (Servicios de Comunicación Enriquecidos) e iMessage para difundir intentos de phishing, empleando tácticas avanzadas como crear enlaces clicables en dispositivos iOS para engañar a los destinatarios y que respondan.

La versión 3 de Darcula, introdujo un panel de administración rediseñado y la aplicación de escritorio Darcula-Suite. Esto permitió a los usuarios crear kits de phishing personalizados, incluso sin conocimientos de programación ni desarrollo web.

Gracias a la integración de IA generativa en las capacidades de darcula los usuarios ahora pueden:

- Generar formularios de phishing (por ejemplo, formularios de recopilación de direcciones) en cualquier idioma.
- Personalizar los campos del formulario, agregando entradas como código postal, correo electrónico y más.
- Traducir automáticamente formularios completos de phishing a idiomas locales, reduciendo tiempo y esfuerzo.
- Mantener el diseño y el estilo visual con una mínima entrada manual.

El proceso es sencillo: Los usuarios proporcionan la URL de una marca o servicio legítimo, y la herramienta visita automáticamente ese sitio web, descarga todos sus recursos y genera una versión editable. Los usuarios pueden inyectar contenido malicioso, como formularios de phishing o campos de captura de credenciales, directamente en la página clonada. Esto crea un sitio web de phishing personalizado y de marca que imita fielmente el sitio real. Esta personalización reduce la eficacia de los métodos de detección tradicionales, lo que requiere enfoques de seguridad dinámicos y basados en el comportamiento para contrarrestar este problema.

3. RECOMENDACIONES:

- Tener cuidado con los mensajes enviados en grupos RCS. Es poco probable que marcas legítimas alerten a los usuarios en estos canales.
- Desconfiar de los mensajes RCS o iMessage provenientes de números o direcciones de correo electrónico desconocidos. Con el cifrado de extremo a extremo, se evita la protección contra estafas de las operadoras telefónicas, por lo que la identificación de mensajes maliciosos depende de la detección en el dispositivo y el reconocimiento humano.

Fuente de Información:	• hxxps://hackread.com/darcula-phishing-kit-uses-ai-to-evade-detection/ • hxxps://www.netcraft.com/blog/ai-enabled-darcula-suite-makes-phishing-kits-more-accessible-easier-to-deploy/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°099	Fecha: 28-04-2025 Página: 5 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el sistema de gestión de contenido Craft CMS		
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:

GitHub, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo inyección de código que afecta al sistema de gestión de contenido "Craft CMS". 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 **crítica** identificada por MITRE como CVE-2025-32432 de tipo inyección de código, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino, no se requiere autenticación.

La vulnerabilidad existe debido a una validación de entrada incorrecta al gestionar solicitudes HTTP. Un atacante remoto no autenticado puede enviar una solicitud HTTP POST especialmente diseñada a la URL "/index.php?p=admin/actions/assets/generate-transform" y ejecutar código PHP arbitrario en el sistema objetivo. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

Los atacantes pueden escanear en busca de identificadores de activos válidos mediante múltiples solicitudes POST. Una vez encontrado un identificador de activo válido, es posible la explotación.

Los scripts de prueba de concepto están disponibles públicamente y automatizan el proceso de búsqueda de identificadores de activos y explotación de la vulnerabilidad. Esta vulnerabilidad está siendo explotado activamente en la naturaleza.

A. Productos afectados:

- Craft CMS: 3.0.0 - 5.6.16.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://github.com/craftcms/cms/blob/3.x/CHANGELOG.md#3915---2025-04-10-critical • hxxps://github.com/craftcms/cms/blob/4.x/CHANGELOG.md#41415---2025-04-10-critical • hxxps://github.com/craftcms/cms/blob/5.x/CHANGELOG.md#5617---2025-04-10-critical • hxxps://github.com/craftcms/cms/commit/e1c85441fa47eeb7c688c2053f25419bc0547b47 • hxxps://github.com/craftcms/cms/security/advisories/GHSA-f3gw-9ww9-jmc3 • hxxps://sensepost.com/blog/2025/investigating-an-in-the-wild-campaign-using-rce-in-craftcms/ • hxxps://craftcms.com/knowledge-base/craft-cms-cve-2025-32432

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°099	Fecha: 28-04-2025 Página: 6 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de escritura fuera de límites en el kernel de Linux		
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:

Linux Foundation ha publicado una vulnerabilidad de severidad **ALTA** de tipo escritura fuera de límites que afecta a todas las versiones en el kernel de Linux. La explotación exitosa de esta vulnerabilidad podría permitir a un a usuario local ejecutar código arbitrario y comprometer el sistema vulnerable.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-53197 de tipo escritura fuera de límites en el kernel de Linux, podría permitir que un usuario local comprometa el sistema afectado. Esta vulnerabilidad puede explotarse localmente, para ello, el atacante tendría que tener acceso físico al sistema de destino para conectar un dispositivo USB malicioso.

La vulnerabilidad existe debido a un error de escritura fuera de límites en las funciones snd_usb_create_quirk(), snd_usb_extigy_boot_quirk(), mbox2_setup_48_24_magic() y snd_usb_mbox2_boot_quirk() de sound/usb/quirks.c. Un usuario local puede activar una escritura fuera de límites y ejecutar código arbitrario en el sistema. Esta vulnerabilidad viene siendo explotado activamente contra dispositivos Android.

A. Productos afectados:

- Kernel de Linux: todas las versiones.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Restringir el acceso físico, hasta que se aplique el parche completo, limitar el acceso físico a los sistemas, especialmente a aquellos expuestos a dispositivos USB no confiables.
- Monitorear la explotación, dada la explotación activa, monitorear los sistemas para detectar actividad sospechosa en dispositivos USB y aplicar protecciones adicionales en los puntos finales cuando sea posible.

Fuente de Información:	• hxxps://git.kernel.org/stable/c/0b4ea4bfe16566b84645ded1403756a2dc4e0f19 • hxxps://git.kernel.org/stable/c/379d3b9799d9da953391e973b934764f01e03960 • hxxps://git.kernel.org/stable/c/62dc01c83fa71e10446ee4c31e0e3d5d1291e865 • hxxps://git.kernel.org/stable/c/920a369a9f014f10ec282fd298d0666129379f1b • hxxps://git.kernel.org/stable/c/9887d859cd60727432a01564e8f91302d361b72b • hxxps://git.kernel.org/stable/c/9b8460a2a7ce478e0b625af7c56d444dc24190f7 • hxxps://git.kernel.org/stable/c/b521b53ac6eb04e41c03f46f7fe452e4d8e9bcca • hxxps://git.kernel.org/stable/c/b8f8b81dabe52b413fe9e062e8a852c48dd0680d • hxxps://git.kernel.org/stable/c/b909df18ce2a998afef81d58bbd1a05dc0788c40 • hxxps://securitylab.amnesty.org/latest/2025/02/cellebrite-zero-day-exploit-used-to-target-phone-of-student-activist/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°099	Fecha: 28-04-2025 Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en productos SAP SE		
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:

SAP SE ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo subida sin restricciones de ficheros de tipos peligrosos, que afecta específicamente a la herramienta Visual Composer y al servicio Universal Description, Discovery and Integration (UDDI) en SAP NetWeaver Application Server Java (AS Java). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto comprometa el sistema vulnerable.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-31324 de tipo subida sin restricciones de ficheros de tipos peligrosos, podría permitir a un atacante remoto comprometa el sistema vulnerable. La falla se debe a la falta de comprobaciones de autenticación y autorización en dos componentes:

La falla se debe a la falta de comprobaciones de autenticación y autorización en dos componentes: El componente Metadata Uploader de Visual Composer, que carece de la autorización adecuada, permite que atacantes no autenticados carguen archivos maliciosos (por ejemplo, webshells JSP) en el sistema host y ejecuten comandos con privilegios administrativos.

El servicio UDDI, que está expuesto sin autenticación, lo que permite a los atacantes leer, modificar o eliminar entradas de servicio de forma remota sin necesidad de iniciar sesión e tipos peligrosos podría permitir a un atacante remoto comprometa el sistema vulnerable.

A. Productos afectados:

- SAP NetWeaver: 7.50.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Reducir la exposición a través de la restricción del acceso a la red de los servicios de SAP NetWeaver.
- Monitorear activa y continuamente los sistemas.

Fuente de Información:	• hxxps[:]//accounts[.]sap[.]com/saml2/idp/sso; • hxxps[:]//support[.]sap[.]com/en/my-support/knowledge-base/security-notes-news/april-2025.html; • hxxps[:]//reliaquest[.]com/blog/threat-spotlight-reliaquest-uncovers-vulnerability-behind-sap-netweaver-compromise/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°099	Fecha: 28-04-2025 Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica 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 Software Foundation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo ejecución remota de código que afecta al producto Apache Tomcat. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante cargar un archivo de sesión serializado malicioso en un directorio escribible a través de solicitudes PUT parciales.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-24813 de tipo ejecución remota de código, podría permitir a un atacante cargar un archivo de sesión serializado malicioso en un directorio escribible a través de solicitudes PUT parciales. Cuando el servidor posteriormente deserializa este archivo (activado por una solicitud HTTP diseñada), se produce la ejecución de código arbitrario.

A. Productos afectados:

- Apache Tomcat: 9.0.0-M1 - 9.0.98.
- Apache Tomcat: 10.0.0-M1 - 10.0.27.
- Apache Tomcat: 10.1.0-M1 - 10.1.34.
- Apache Tomcat: 11.0.0-M1 - 11.0.2.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad. Apache Tomcat corrigió esta vulnerabilidad en las versiones 11.0.3, 10.1.35 y 9.0.99.

Fuente de Información:	• hxxps[:]//lists[.]apache[.]org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq; • hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/10/5; • hxxps[:]//www[.]vicarious[.]io/vsociety/posts/cve-2025-24813-detect-apache-tomcat-rce. • hxxps[:]//www[.]vicarious[.]io/vsociety/posts/cve-2025-24813-mitigate-apache-tomcat-rce

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°099	Fecha: 28-04-2025
		Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de agotamiento de recursos en IBM DataPower Gateway		
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:

IBM Corporation ha publicado una vulnerabilidad de severidad **ALTA** de tipo agotamiento de recursos que afecta a varias versiones de IBM DataPower Gateway. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado realizar un ataque de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2021-38872 de tipo agotamiento de recursos en IBM DataPower Gateway, podría permitir a un atacante remoto no autenticado realizar un ataque de DoS al consumir recursos a través de múltiples solicitudes. El vector de ataque basado en red, no requiere interacción ni privilegios del usuario.

La vulnerabilidad existe porque la aplicación no controla adecuadamente el consumo de recursos internos. Un atacante remoto puede provocar el agotamiento de recursos y realizar un ataque de DoS.

A. Productos afectados:

- IBM DataPower Gateway: 10.0.1.0 - 10.0.1.4, 10.0.2.0, 10.0.3.0, 2018.4.1.0 - 2018.4.1.17.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.ibm.com/support/pages/node/6586704 • hxxps://exchange.xforce.ibmcloud.com/vulnerabilities/208348

Índice alfabético