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

198-2024-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

Google advierte sobre vulnerabilidad de seguridad CVE-2024-7965 en Chrome explotada activamente 4
Vulnerabilidad crítica en Web Application Firewall (WAF) de Hillstone Networks 5
Vulnerabilidad crítica en el Sistema de gestión de la calidad SeaCMS 6
Vulnerabilidad de Apache Kafka en IBM Tivoli Netcool/OMNIbus Transport Module Common Integration Library 7
Índice alfabético 8

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°198	Fecha: 27-08-2024
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Google advierte sobre vulnerabilidad de seguridad CVE-2024-7965 en Chrome explotada activamente		
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:

Google ha revelado que una falla de seguridad que fue reparada como parte de una actualización de software lanzada la semana pasada para su navegador Chrome ha sido explotada activamente. Esta vulnerabilidad ha sido registrada como CVE-2024-7965.

Desde Google alertan de que los piratas informáticos están tomando ventaja con este problema y ponen en riesgo la seguridad y privacidad de los usuarios.

2. DETALLES:

La vulnerabilidad ha sido descrita como un error de implementación inapropiado en el motor JavaScript V8 y WebAssembly.

"Una implementación inadecuada en V8 en Google Chrome anterior a 128.0.6613.84 permitió a un atacante remoto explotar potencialmente la corrupción del montón a través de una página HTML diseñada", según una descripción del error en la Base de Datos Nacional de Vulnerabilidades (NVD) del NIST.

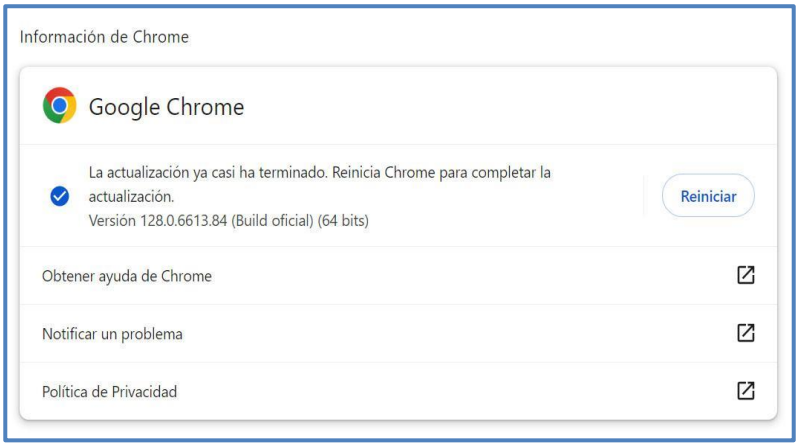
También se afirma que se informó de una explotación indiscriminada de CVE-2024-7965 después de este lanzamiento.

Versiones afectadas:

- Versiones anteriores a 128.0.6613.84.

3. RECOMENDACIONES:

- Actualizar el paquete afectado con la última versión disponible para abordar esta vulnerabilidad, sin importar qué sistema operativo estés utilizando.
- Asegurarse de que tienes la última versión de Google Chrome instalada yendo al menú de arriba a la derecha, ir a Ayuda y hacer clic a Información de Google Chrome, donde automáticamente te mostrará qué versión tienes instalada. En caso de que haya una nueva disponible, empezará a descargarla e instalarla. Se debe reiniciar el navegador, una vez se instale, para completar la actualización.



Fuente de Información:	• hxxps://nvd.nist.gov/vuln/detail/CVE-2024-7965 • hxxps://thehackernews.com/2024/08/google-warns-of-cve-2024-7965-chrome.html • hxxps://www.redeszone.net/noticias/seguridad/google-alerta-fallo-chrome/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°198	Fecha: 27-08-2024 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en Web Application Firewall (WAF) de Hillstone 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:

Hillstone Networks ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo validación de entrada incorrecta en la página del código de verificación del software de Web Application Firewall (WAF). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en los sistemas afectados, lo que podría provocar un compromiso total del sistema.

2. DETALLES:

Un web application firewall (WAF) es un tipo específico de firewall de aplicaciones que filtra, monitorea y bloquea el tráfico HTTP hacia y desde un servicio web. Al inspeccionar el tráfico HTTP, puede prevenir ataques que exploten vulnerabilidades conocidas de una aplicación web, como inyección SQL, cross-site scripting (XSS), inclusión de archivos y configuración inadecuada del sistema.

Hillstone Networks ofrece el Firewall de Aplicaciones Web (WAF) de la Serie W, que proporciona una seguridad integral de clase empresarial para servidores web, aplicaciones y APIs.

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2024-8073 de tipo validación de entrada incorrecta en la página del código de verificación en WAF, podría permitir a un atacante remoto crear solicitudes especialmente diseñadas. Al explotar esta debilidad, los actores maliciosos pueden concatenar comandos y ejecutar código arbitrario, lo que podría tomar el control del servidor que aloja el WAF.

A. Productos afectados:

- Web Application Firewall (WAF): versiones desde 5.5R6-2.6.7 a 5.5R6-2.8.13.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión 5.5R6-2.8.14, que incluye un parche para mitigar la vulnerabilidad identificada. Las organizaciones que utilizan Hillstone WAF deben aplicar el parche rápidamente, monitorear los registros del sistema para detectar actividad sospechosa y considerar medidas de seguridad adicionales como sistemas de detección de intrusiones (IDS) y escáneres de seguridad de aplicaciones web.

Fuente de Información:	• hxxps://www.hillstonenet.com.cn/security-notification/2024/08/21/mlzrld-2/ • hxxps://talkback.sh/vulnerability/CVE-2024-8073 • hxxps://securityonline.info/hillstone-networks-addresses-critical-rce-vulnerability-in-waf-cve-2024-8073-cvss-9-8/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°198	Fecha: 27-08-2024 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en el Sistema de gestión de la calidad SeaCMS		
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 reportado una vulnerabilidad de severidad **CRÍTICA** de tipo inyección SQL en el Sistema de gestión de la calidad SeaCMS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar comandos SQL arbitrarios, lo que provocaría un acceso no autorizado a la base de datos, robo de datos, manipulación de datos y posible compromiso del sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2024-41444 de tipo inyección SQL en el parámetro clave de /js/player/dmplayer/dmku/index.php?ac=so. La manipulación del argumento key con una entrada desconocida conduce a una vulnerabilidad de inyección SQL. Un ataque exitoso podría permitir a un atacante remoto ejecutar comandos SQL arbitrarios, lo que provocaría un acceso no autorizado a la base de datos, robo de datos, manipulación de datos y posible compromiso del sistema.

El producto construye todo o parte de un comando SQL utilizando una entrada influenciada externamente desde un componente ascendente, pero no neutraliza o neutraliza incorrectamente elementos especiales que podrían modificar el comando SQL deseado cuando se envía a un componente descendente. Se ven afectados la confidencialidad, la integridad y la disponibilidad.

A. Productos afectados:

- SeaCMS v12.9.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Implementar la validación y el saneamiento de entrada para toda la entrada proporcionada por el usuario, especialmente en el archivo afectado /js/player/dmplayer/dmku/index.php.
- Utilizar declaraciones preparadas con consultas parametrizadas para evitar la inyección de SQL.
- Aplicar el principio del mínimo privilegio a las cuentas de base de datos utilizadas por la aplicación.
- Implementar firewalls de aplicaciones web (WAF) para ayudar a detectar y bloquear los intentos de inyección de SQL.
- Auditar y revisar periódicamente los registros de acceso a la base de datos para detectar actividades sospechosas.
- Considerar el uso de servidores proxy de base de datos o middleware que puedan detectar y prevenir los intentos de inyección de SQL.

Fuente de Información:	• hxxps://gist.github.com/looppppp/fa328c81ce19c1097d10f95c763d0d50 • hxxps://github.com/seacms-net/CMS • hxxps://vuldb.com/?id.275846

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°198	Fecha: 27-08-2024 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de Apache Kafka en IBM Tivoli Netcool/OMNIbus Transport Module Common Integration Library		
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 reportado una vulnerabilidad de severidad **ALTA** de tipo Autorización incorrecta en la plataforma Apache Kafka en IBM Tivoli Netcool/OMNIbus Transport Module Common Integration Library. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto provocar una condición de denegación de servicio (DoS).

2. DETALLES:

Apache Kafka (Kafka) es una plataforma de transmisión distribuida de código abierto que permite (entre otras cosas) el desarrollo de aplicaciones impulsadas por eventos en tiempo real. Apache Kafka es un proyecto de intermediación de mensajes de código abierto desarrollado por LinkedIn y donado a la Apache Software Foundation escrito en Java y Scala.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-27309 de tipo Autorización incorrecta, podría permitir a un atacante remoto obtener acceso a información confidencial y modificar datos del sistema. La vulnerabilidad existe porque la aplicación no controla adecuadamente el consumo de recursos internos. Un atacante remoto puede obtener acceso a información confidencial y modificar datos del sistema.

Apache Kafka es utilizado por IBM Tivoli Netcool/OMNIbus Transport Module Common Integration Library, es vulnerable a un ataque de DoS, causada por un control de acceso inadecuado durante la migración del modo ZK al modo KRaft. Al enviar una solicitud especialmente diseñada, un atacante remoto podría aprovechar esta vulnerabilidad para provocar una condición de DoS.

A. Productos afectados:

- IBM Tivoli Netcool/OMNIbus Integration – Transport Module Common Integration Library: 18.0 - 39.0.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://www.ibm.com/support/pages/node/7161416 • hxxps://exchange.xforce.ibmcloud.com/vulnerabilities/287552 • hxxps://cve.org/CVERecord?id=CVE-2024-27309

Índice alfabético

Explotación de vulnerabilidades conocidas 4, 5, 6, 7