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

243-2024-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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°243	Fecha: 21-10-2024
		Página: 4 de 11

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Más de 6.000 sitios de WordPress hackeados para instalar plugins que impulsan a los ladrones de información		
Tipo de Ataque	Stealers		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:

En los últimos años, el malware que roba información (info stealer) se ha convertido en un flagelo para los defensores de la seguridad en todo el mundo, ya que las credenciales robadas se utilizan para violar redes y robar datos.

Desde 2023, se utiliza una campaña maliciosa llamada ClearFake para mostrar mensajes falsos de actualización del navegador web en sitios web comprometidos que distribuyen malware para robar información.

En 2024, se introdujo una nueva campaña llamada ClickFix que comparte muchas similitudes con ClearFake, pero que en cambio pretende ser mensajes de error de software con correcciones incluidas. Sin embargo, estas "correcciones" son scripts de PowerShell que, cuando se ejecutan, descargan e instalan malware para robar información.

2. DETALLES:

La semana pasada, GoDaddy informó que los actores de amenazas ClearFake/ClickFix han violado más de 6.000 sitios de WordPress para instalar complementos maliciosos que muestran alertas falsas asociadas con estas campañas.

"El equipo de seguridad de GoDaddy está rastreando una nueva variante del malware de actualización de navegador falso ClickFix (también conocido como ClearFake) que se distribuye a través de complementos falsos de WordPress", explica el investigador de seguridad de GoDaddy, Denis Sinegubko.

"Estos complementos aparentemente legítimos están diseñados para parecer inofensivos a los administradores de sitios web, pero contienen scripts maliciosos incorporados que envían mensajes falsos de actualización del navegador a los usuarios finales".

Los complementos maliciosos utilizan nombres similares a los complementos legítimos, como Wordfense Security y LiteSpeed Cache, mientras que otros usan nombres genéricos e inventados.

La lista de complementos maliciosos observados en esta campaña entre junio y septiembre de 2024 son:

- LiteSpeed Cache Classic
- Custom CSS Injector
- MonsterInsights Classic

- Custom Footer Generator
- Wordfence Security Classic
- Custom Login Styler
- Search Rank Enhancer
- Dynamic Sidebar Manager
- SEO Booster Pro
- Easy Themes Manager
- Google SEO Enhancer
- Form Builder Pro
- Rank Booster Pro
- Quick Cache Cleaner
- Admin Bar Customizer
- Responsive Menu Builder
- Advanced User Manager
- SEO Optimizer Pro
- Advanced Widget Manage
- Simple Post Enhancer
- Content Blocker
- Social Media Integrator

La empresa de seguridad web Sucuri también señaló que un complemento falso llamado "Universal Popup Plugin" también es parte de esta campaña.

Una vez instalado, el complemento malicioso conectará varias acciones de WordPress según la variante para inyectar un script JavaScript malicioso en el HTML del sitio.

```
<script type="text/javascript" src="https://[infected.site]t/wp-
content/plugins/custom-css-injector/cci-script.js" id="custom-css-injector-js">
</script>
```

Cuando se carga, este script intentará cargar otro archivo JavaScript malicioso almacenado en un contrato inteligente de Binance Smart Chain (BSC), que luego carga el script ClearFake o ClickFix para mostrar los banners falsos.

Según los registros de acceso al servidor web analizados por Sinegubko, los actores de amenazas parecen estar utilizando credenciales de administrador robadas para iniciar sesión en el sitio de WordPress e instalar el complemento de manera automática.

Los actores de amenazas inician sesión mediante una única solicitud POST HTTP en lugar de visitar primero la página de inicio de sesión del sitio. Esto indica que se está haciendo de forma automatizada una vez que ya se han obtenido las credenciales. Una vez que el actor de la amenaza inicia sesión, carga e instala el complemento malicioso.

```
190.124.190.XX - - [02/Sep/2024:01:15:22 -0700] "POST /wp-login.php HTTP/1.1" 302 -
"-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/128.0.0.0 Safari/537.36" 1412 **1/1412064**

190.124.190.XX - - [02/Sep/2024:01:15:24 -0700] "GET /wp-admin/ HTTP/1.1" 200 118965
"-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/128.0.0.0 Safari/537.36" 4187 **4/4187620**

190.124.190.XX - - [02/Sep/2024:01:15:30 -0700] "GET /wp-admin/plugin-install.php
HTTP/1.1" 200 37714 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36" 2020
**2/2020584**

190.124.190.XX - - [02/Sep/2024:01:15:32 -0700] "POST /wp-admin/update.php?
action=upload-plugin HTTP/1.1" 200 28720 "https://[redacted]/wp-admin/plugin-
install.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36" 9869 **9/9869469**

190.124.190.XX - - [02/Sep/2024:01:15:43 -0700] "GET /wp-admin/plugins.php?
action=activate&plugin=quick-cache-cleaner%2Findex.php&_wpnonce=588b765730 HTTP/1.1"
302 - "https://[redacted]/wp-admin/plugin-install.php" "Mozilla/5.0 (Macintosh;
Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0
Safari/537.36" 3913 **3/3913918**
```

Si bien no está claro cómo los actores de amenazas obtienen las credenciales, el investigador señala que podría ser a través de ataques previos de fuerza bruta, phishing y malware de robo de información.

3. RECOMENDACIONES:

- Examinar inmediatamente la lista de complementos instalados y eliminar los que no haya instalado usted mismo.
- Restablecer inmediatamente las contraseñas de los usuarios administradores a una contraseña única que solo se usa en su sitio.
- Aplicar políticas de contraseñas seguras. Cambiar las contraseñas de todas sus cuentas de manera periódica utilizando una contraseña única para cada sitio, y permanecer alerta ante posibles intentos de phishing.
- Limitar la tasa de intentos y fallas de autenticación.
- Hacer uso del doble factor de autentificación.
- Aplicar parches y actualizar periódicamente el software y las aplicaciones a su última versión, así como realizar evaluaciones de vulnerabilidad periódicas.
- Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados. Estos programas pueden detectar y eliminar ransomware y otro software malicioso antes de que puedan cifrar sus archivos.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Capacitar a su equipo en las mejores prácticas de ciberseguridad y manténgalos informados sobre las últimas amenazas.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/over-6-000-wordpress-hacked-to-install-plugins-pushing-infostealers/ • hxxps://blog.segu-info.com.ar/2024/10/sitios-de-wordpress-modificados-para.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°243	Fecha: 21-10-2024 Página: 7 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Microsoft Edge		
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 ha publicado una vulnerabilidad de severidad **MEDIA** de tipo suplantación de identidad en Microsoft Edge (basado en Chromium). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir las políticas de seguridad.

2. **DETALLES:**

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-43577 de tipo suplantación de identidad en Microsoft Edge (basado en Chromium), podría permitir a un atacante remoto no autenticado eludir las políticas de seguridad. Un atacante podría alojar un sitio web especialmente diseñado para explotar la vulnerabilidad a través de Microsoft Edge y luego convencer a un usuario para que visite el sitio web. Sin embargo, el atacante tendría que enviar a la víctima un archivo malicioso que ésta tendría que ejecutar.

Un atacante que usa una página especialmente diseñada o un script de contenido inyectado en cualquier página puede mostrar la ventana emergente de una extensión sobre un mensaje de permiso o un cuadro de diálogo para compartir pantalla, lo que permite que la extensión falsifique partes de la interfaz de usuario del mensaje que muestran el origen.

A. **Productos afectados:**

- Microsoft Edge, versiones anteriores a 130.0.2849.46.

3. **RECOMENDACIÓN:**

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

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43577

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°243	Fecha: 21-10-2024 Página: 8 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en la línea de productos HikCentral de HikVision		
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 múltiples vulnerabilidades de severidad **ALTA** de tipo inyección SQL y Cross Site Scripting (XSS) en la serie de productos HikCentral de HikVision Digital Technology CO., Ltd. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado generar comandos ejecutables en el archivo CSV y ejecutar consultas SQL arbitrarias.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-47485 de tipo inyección de CSV en algunas versiones de HikCentral Master Lite, podría permitir a un atacante crear datos maliciosos para generar comandos ejecutables en el archivo CSV.

La vulnerabilidad de severidad **baja** identificada por MITRE como CVE-2024-47486 de tipo XSS en algunas versiones de HikCentral Master Lite, podría permitir a un atacante inyectar scripts en ciertas páginas creando datos maliciosos.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-47487 de tipo inyección SQL en algunas versiones profesionales de HikCentral, podría permitir que un usuario autenticado ejecute consultas SQL arbitrarias.

A. Productos afectados:

- HikCentral Master Lite, versiones anteriores a 2.3.0.
- HikCentral Profesional, versiones anteriores a 2.6.1.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.hikvision.com/en/support/cybersecurity/security-advisory/security-vulnerabilities-in-hikcentral-product-series/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°243	Fecha: 21-10-2024 Página: 9 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Nice Backgrounds de Brx8r.		
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 carga sin restricciones de archivos de tipo peligroso en Nice Backgrounds de brx8r. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado cargar un shell web en un servidor web.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-49330 de tipo carga sin restricciones de archivos de tipo peligroso en Nice Backgrounds de brx8r, podría permitir a un atacante cargar un shell web en un servidor web. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante cargar archivos maliciosos (shells web) al servidor web afectado. Un atacante podría ejecutar código arbitrario en el servidor, obtener acceso no autorizado a información confidencial almacenada en el servidor, manipular o eliminar archivos, lo que provocaría interrupciones del servicio y realizar un movimiento lateral a través del servidor comprometido para atacar otros sistemas en la red.

A. Productos afectados:

- Nice Backgrounds, versiones hasta la 1.0 en WordPress.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Implementar restricciones estrictas de tamaño y tipo de archivo en todas las funcionalidades de carga de archivos.
- Realizar una validación exhaustiva del lado del servidor de todos los archivos cargados, incluida la verificación del tipo MIME y el análisis del contenido de los archivos.
- Implementar o configurar un Firewall de aplicaciones web (WAF) para detectar y bloquear intentos maliciosos de carga de archivos.
- Asegurarse de que el proceso del servidor web se ejecute con los permisos mínimos necesarios.
- Aislar los sistemas que ejecutan Nice Backgrounds de los segmentos de red críticos.
- Realizar escaneos de vulnerabilidad y pruebas de penetración frecuentes para detectar cualquier explotación exitosa.
- Implementar un registro y monitoreo robusto para las actividades de carga de archivos y comportamientos inusuales del servidor.

Fuente de Información:	• hxxps://www.tenable.com/cve/CVE-2024-49330 • hxxps://www.cisa.gov/news-events/bulletins/sb24-295

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°243	Fecha: 21-10-2024 Página: 10 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Adobe Commerce y Magento Open Source		
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:

Magento, Inc. Adobe ha publicado una vulnerabilidad de severidad **ALTA** de tipo inyección de entidad externa XML en Adobe Commerce (anteriormente Magento Commerce) y Magento Open Source. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución de código arbitrario, la omisión de la función de seguridad y la ampliación de privilegios.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-34102 de tipo inyección de entidad externa XML en Adobe Commerce y Magento Open Source, podría permitir a un atacante remoto comprometer la aplicación afectada. La vulnerabilidad existe debido a una validación insuficiente de la entrada XML proporcionada por el usuario. Un atacante remoto puede pasar un código XML especialmente diseñado a la aplicación afectada y ver el contenido de archivos arbitrarios en el sistema o iniciar solicitudes a sistemas externos.

A. Productos afectados:

- Adobe Commerce: 2.3.0 - 2.3.7-p4-ext-7, 2.4.0 - 2.4.7-beta2, 2.2.0 - 2.2.11, 2.0.0 - 2.0.18, 2.1.0 - 2.1.18.
- Magento Open Source: 2.4.0 - 2.4.7-beta2, 2.3.0 - 2.3.7-p4, 2.2.0 - 2.2.11, 2.1.0 - 2.1.18, 2.0.0 - 2.0.18.
- Plug-in Adobe Commerce Webhooks: 1.2.0 a 1.4.0.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://helpx.adobe.com/security/products/magento/apsb24-40.html

Índice alfabético