PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 22 de marzo de 2024

071-2024-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 Aérea del 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 las empresas 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

Nuevos ataques de phishing de StrelaStealer afectan a más de 100 organizaciones en la UE y EE. UU. 4
Vulnerabilidad crítica en el servicio Apache Airflow de AWS Managed Workflows 5
Vulnerabilidades críticas en productos DELL 6
Vulnerabilidades en el servidor VNC integrado de QEMU 7
Actualización de Fedora 39 para la configuración de Apache Commons 8
Vulnerabilidad en WebAccess/SCADA de Advantech 9
Índice alfabético 10

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°071	Fecha: 22-03-2024
		Página: 4 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Nuevos ataques de phishing de StrelaStealer afectan a más de 100 organizaciones en la UE y EE. UU.		
Tipo de Ataque	Stealers	Abreviatura	Stealers
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C03
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

En un informe recién publicado, investigadores de Palo Alto Networks Unit 42 han revelado una preocupante tendencia en el mundo de la ciberseguridad: una nueva oleada de ataques de phishing que tiene como objetivo a más de 100 organizaciones en la Unión Europea y Estados Unidos. Estos ataques buscan desplegar un moderno ladrón de información conocido como StrelaStealer.

2. DETALLES:

Estas campañas vienen en forma de correos electrónicos no deseados con archivos adjuntos que eventualmente lanzan la carga útil DLL de StrelaStealer.

En un intento de evadir la detección, los atacantes cambian el formato del archivo adjunto inicial del correo electrónico de una campaña a la siguiente, para evitar ser detectados por los sistemas de seguridad. Este enfoque ingenioso les ha permitido burlar las firmas y patrones de detección utilizados anteriormente.

StrelaStealer tiene la capacidad de extraer los datos de inicio de sesión del correo electrónico de clientes de correo destacados y transferirlos a un servidor bajo el control del atacante.

Desde entonces, se han detectado dos campañas a gran escala relacionadas con el malware en noviembre de 2023 y enero de 2024 dirigidas a los sectores de alta tecnología, finanzas, profesional y legal, manufactura, gobierno, energía, seguros y construcción en la Unión Europea y los Estados Unidos.

Estos ataques también pretenden difundir una nueva variante del stealer, que está equipada con tácticas de ofuscación mejoradas y sistemas antianálisis. Esta variante se propaga a través de correos electrónicos con temática de facturas y archivos ZIP adjuntos, lo que supone un cambio con respecto a los anteriores archivos ISO.

Dentro de los archivos ZIP se encuentra un archivo JavaScript que coloca un archivo por lotes, que, a su vez, lanza la carga útil DLL ladrón usando rundll32.exe, un componente legítimo de Windows responsable de ejecutar bibliotecas de enlaces dinámicos de 32 bits.

El malware stealer también emplea una colección de técnicas de ofuscación para complicar el análisis en entornos aislados. "Con cada nueva oleada de campañas de correo electrónico, los autores de la amenaza modifican tanto el archivo adjunto, que desencadena la cadena de infección, como la propia carga DLL", señalan los investigadores.

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos ni descargar archivos adjuntos de fuentes desconocidas.
- Verificar la fuente de información de tus correos entrantes.
- Mantener el software actualizado. Actualizar periódicamente los sistemas operativos, las aplicaciones y el software de seguridad para corregir las vulnerabilidades.
- Implementar soluciones de seguridad integrales que puedan detectar y bloquear malware.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://thehackernews.com/2024/03/new-strelastealer-phishing-attacks-hit.html • hxxps://devel.group/blog/nueva-ola-de-ataques-de-phishing-golpea-a-mas-de-100-organizaciones-en-la-union-europea-y-estados-unidos/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°071**	**Fecha: 22-03-2024**
		Página: 5 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en el servicio Apache Airflow de AWS Managed Workflows		
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:

Tenable Research ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo fijación de sesiones y las secuencias de comandos entre sitios (XSS) en el servicio AWS Managed Workflows para Apache Airflow (MWAA), al que se ha denominado "FlowFixation". La explotación exitosa de esta vulnerabilidad podría permitir la toma completa del panel de administración web de la instancia de Airflow de la víctima.

2. DETALLES:

Apache Airflow es una plataforma de código abierto para crear, programar y monitorear flujos de trabajo mediante programación. MWAA es un servicio administrado de AWS que simplifica la configuración, implementación y escalado de dichos flujos de trabajo de datos. Permite a los usuarios crear, programar y monitorear sus flujos de trabajo en un Apache Airflow administrado sin administrar la infraestructura subyacente.

Los investigadores de Tenable Research, han descubierto una vulnerabilidad denominada “FlowFixation”, que podría haber permitido a un actor malicioso secuestrar la sesión de una víctima en MWAA y que podría haber resultado en la ejecución remota de código (RCE) en la instancia subyacente, y en movimiento lateral hacia otros servicios.

La vulnerabilidad de apropiación de cuenta “FlowFixation”, ahora solucionada por Amazon Web Services (AWS), resulta de una combinación de fijación de sesión en el panel de administración web de AWS MWAA junto con una mala configuración del dominio de Amazon AWS que conduce a XSS. Al abusar de la vulnerabilidad, un atacante podría haber obligado a las víctimas a utilizar y autenticar la sesión conocida del atacante. Esta manipulación podría haber permitido al atacante utilizar posteriormente la misma sesión, ahora autenticada, para hacerse cargo del panel de administración web de la víctima.

La interfaz de usuario de Airflow es un panel web de administración que requiere autenticación de AWS IAM.

Las investigaciones adicionales revelaron que, numerosos dominios de servicios compartidos en AWS, Azure y GCP estaban mal configurados, lo que ponía a los clientes de la nube en un riesgo considerable. Algunos riesgos importantes debido a la mala configuración incluyeron el lanzamiento de cookies, lo que puede provocar un abuso de fijación de sesión y una omisión de protección contra falsificación de solicitudes entre sitios (CSRF); y omisión de protección de cookies en el mismo sitio.

Agregar los dominios mal configurados a la Lista pública de sufijos (PSL) habría evitado la explotación de FlowFixation y otras vulnerabilidades, incluidas vulnerabilidades de alta gravedad que otros han documentado y divulgado.

A. Productos afectados:

- Servicio Apache Airflow de AWS Managed Workflows.

3. RECOMENDACIONES:

- Asegurarse de que las configuraciones en la nube sean seguras y auditarlas periódicamente para evitar que sean explotadas por un actor de amenazas.
- Contribuir a proteger sus datos y aplicaciones, a pesar de que los CSP sean responsables de la seguridad de la nube.
- Colaborar para fortalecer sus defensas contra amenazas cibernéticas cada vez más sofisticadas.

Fuente de Información:	• hxxps://www.tenable.com/blog/flowfixation-aws-apache-airflow-service-takeover-vulnerability-and-why-neglecting-guardrails

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°071**	**Fecha: 22-03-2024**
		Página: 6 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades críticas en productos DELL		
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 dos vulnerabilidades de severidad **CRÍTICA** y **MEDIA** de tipo omisión faltante para función crítica y neutralización inadecuada de secuencias CRLF en encabezados HTTP (División de solicitud/respuesta HTTP) en productos DELL. La explotación exitosa de esta vulnerabilidad podría provocar la pérdida de la confidencialidad, integridad y disponibilidad.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2023-34329 de tipo omisión faltante para función crítica, puede provocar una omisión de autenticación falsificando el encabezado HTTP. Una explotación exitosa de esta vulnerabilidad puede provocar la pérdida de confidencialidad, integridad y disponibilidad.

Se ha asignado el siguiente identificador para la vulnerabilidad de severidad **media**: CVE-2023-34472.

A. Productos afectados:

- Z9432F-ON *firmware,* versiones anteriores a la v3.51.5.1-18.
- S5448F-ON *firmware*, versiones anteriores a la v3.52.5.1-10.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión 3.52.5.1-10 o posterior disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://www.dell.com/support/kbdoc/es-es/000223381/dsa-2024-148-security-update-for-dell-networking-z9432f-on-and-s5448f-on-for-multiple-vulnerabilities

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°071**	**Fecha: 22-03-2024**
		Página: 7 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en el servidor VNC integrado de QEMU		
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 **MEDIA** de tipo desreferencia del puntero NULO (NULL) en el servidor VNC integrado de QEMU. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario remoto realizar un ataque de denegación de servicio (DoS).

2. **DETALLES:**

   VNC (Virtual Network Computing) es una tecnología que permite controlar de forma remota un sistema informático. En el contexto de QEMU, que es un software de virtualización, el uso de VNC puede ser muy útil para interactuar con las máquinas virtuales que se ejecutan dentro de QEMU de forma remota.

   La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2023-6683 de tipo desreferencia del puntero NULO, existe debido a un error de desreferencia del puntero NULL al procesar mensajes ClientCutText dentro del servidor VNC integrado de QEMU. Un cliente VNC autenticado remoto puede pasar datos especialmente diseñados a la aplicación y realizar un ataque de DoS.

   Una desreferencia de puntero NULL ocurre cuando la aplicación desreferencia un puntero que espera que sea válido, pero es NULL, lo que generalmente provoca un bloqueo o una salida.

   A. Productos afectados:

   - QEMU: todas las versiones.

3. **RECOMENDACIÓN:**

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

Fuente de Información:	• hxxp://bugzilla.redhat.com/show_bug.cgi?id=2254825

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°071	Fecha: 22-03-2024
		Página: 8 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Actualización de Fedora 39 para la configuración de Apache Commons		
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 la actualización de dos vulnerabilidades de severidad **ALTA** de tipo escritura fuera de límites para la configuración de Apache Commons. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema objetivo.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-29131 de tipo escritura fuera de límites, existe debido a un error de límite al procesar entradas que no son de confianza. Un atacante remoto puede pasar datos especialmente diseñados a la aplicación, provocar una escritura fuera de límites y ejecutar código arbitrario en el sistema objetivo.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-29133 de tipo escritura fuera de límites, existe debido a un error de límite al llamar a ListDelimiterHandler.flatten(Object, int) con un árbol de objetos cíclico. Un atacante remoto puede pasar entradas especialmente diseñadas a la aplicación, desencadenar una escritura fuera de límites y ejecutar código arbitrario en el sistema objetivo.

A. Productos afectados:

- Fedora: 39.
- Apache-commons-configuration: antes de 2.10.1-1.fc39.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://bodhi.fedoraproject.org/updates/FEDORA-2024-fa7b758114

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°071	Fecha: 22-03-2024
		Página: 9 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en WebAccess/SCADA de Advantech		
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 neutralización inadecuada de elementos especiales utilizados en un comando SQL (Inyección SQL) en WebAccess/SCADA de Advantech. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante autenticado leer o modificar una base de datos remota.

2. DETALLES:

WebAccess/SCADA es una plataforma de software desarrollada por Advantech, una empresa global de tecnología que se especializa en hardware y software para la automatización industrial y la informática embebida. WebAccess/SCADA es un sistema de control y adquisición de datos (SCADA) que permite supervisar, controlar y recopilar datos de procesos industriales en tiempo real a través de una interfaz web.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-2453 de tipo inyección SQL, podría permitir a un atacante autenticado inyectar remotamente código SQL en la base de datos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante leer o modificar datos en la base de datos remota.

A. Productos afectados:

- WebAccess/SCADA, versión 9.1.5U.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión 9.1.6 o superior disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-081-01

Índice alfabético

Explotación de vulnerabilidades conocidas 5, 6, 7, 8, 9
Stealers 4