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, 09 de febrero de 2024

035-2024-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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°035	Fecha: 09-02-2024
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	FortiOS y FortiProxy: Múltiples Vulnerabilidades en Fortinet		
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**:

Fortinet ha informado de 3 vulnerabilidades, 2 críticas y 1 media, que afectan a su sistema operativo FortiOS, una de ellas reportada por Gwendal Guégniaud (CVE-2024-23113). La explotación de éstas podría permitir a un atacante ejecutar código o comandos no autorizados.

2. **DETALLES:**

Esta vulnerabilidad de escritura fuera de límites en sslvpnd podría permitir a un atacante remoto, no autenticado, ejecutar código o comandos arbitrarios a través de peticiones HTTP especialmente diseñadas. Se ha asignado el identificador CVE-2024-21762 para esta vulnerabilidad.

Una vulnerabilidad en el uso de cadenas de formato controladas externamente en el demonio fgfmd podría permitir a un atacante remoto, no autenticado, ejecutar código arbitrario o comandos a través de peticiones especialmente diseñadas. Se ha asignado el identificador CVE-2024-23113 para esta vulnerabilidad.

La vulnerabilidad enumerada como CVE-2023-44487 corresponde a un HTTP/2 Rapid Reset Attack. El protocolo HTTP/2 permite una denegación de servicio (consumo de recursos del servidor) porque la cancelación de solicitudes puede restablecer muchas transmisiones rápidamente.

Actualmente se conoce que la vulnerabilidad CVE-2024-21762 está siendo potencialmente explotada. Sin embargo, se desconoce la disponibilidad de exploits que aprovechen estas vulnerabilidades, así como tampoco se han publicado pruebas de concepto (PoC) sobre los detalles del fallo publicado.

Recursos Afectados:

Las siguientes versiones de FortiOS están afectadas:

- FortiOS desde 7.4.0 hasta 7.4.2.
- FortiOS desde 7.2.0 hasta 7.2.6.
- FortiOS desde 7.0.0 hasta 7.0.13.
- FortiOS desde 6.4.0 hasta 6.4.14.
- FortiOS desde 6.2.0 hasta 6.2.15.
- FortiOS todas las versiones 6.0.

Las siguientes versiones de FortiProxy están afectadas:

- Fortiproxy desde 7.4.0 a 7.4.1.
- Fortiproxy desde 7.2.0 a 7.2.7.
- Fortiproxy desde 7.0 todas las versiones.

3. RECOMENDACIONES:

- Actualizar a FortiOS versión 7.4.3 o superior (para las versiones desde 7.4.0 hasta 7.4.2).
- Actualizar a FortiOS versión 7.2.7 o superior (para las versiones desde 7.2.0 hasta 7.2.6).
- Actualizar a FortiOS versión 7.0.14 o superior (para las versiones desde 7.0.0 hasta 7.0.13).
- Actualizar a FortiOS versión 6.4.15 o superior (para las versiones desde 6.4.0 hasta 6.4.14).
- Actualizar a FortiOS versión6.2.16 o superior (para las versiones desde 6.2.0 hasta 6.2.15).
- Migrar a una versión fija (para todas las versiones 6.0 de FortiOS).
- Actualice a Fortiproxy versión 7.4.2 o superior (para las versiones desde 7.4.0 a 7.4.1).
- Actualice a Fortiproxy versión 7.2.8 o superior (para las versiones desde 7.2.0 a 7.2.7)
- Migrar a una versión fija (para todas las versiones 7.0 de FortiProxy).
- Deshabilitar SSL VPN en caso no pueda aplicar los parches (deshabilitar el modo web NO es una solución alternativa válida).
- Eliminar la compatibilidad con HTTP/2 con modo proxy con inspección SSL.

Fuente de Información:	• hxxps://www.fortiguard.com/psirt/FG-IR-24-015 • hxxps://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-fortios-de-fortinet • hxxps://www.ccn-cert.cni.es/es/seguridad-al-dia/avisos-ccn-cert/12896-ccn-cert-av-02-24-actualizaciones-de-seguridad-para-productos-fortinet.html • hxxps://www.fortiguard.com/psirt/FG-IR-23-397

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°035**	**Fecha: 09-02-2024**
		Página: 6 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en múltiples versiones de PostgreSQL		
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 errores de caída/reducción de privilegios en múltiples versiones del sistema de gestión de bases de datos PostgreSQL. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución de código arbitrario.

2. DETALLES:

PostgreSQL es un sistema de gestión de bases de datos relacional de código abierto que se destaca por su robustez, extensibilidad y cumplimiento de los estándares SQL.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-0985 se debe a una caída tardía de privilegios en ACTUALIZAR VISTA MATERIALIZADA CONCURRENTE en PostgreSQL permite a un creador de objetos ejecutar funciones SQL arbitrarias como emisor de comandos. El comando pretende ejecutar funciones SQL como propietario de la vista materializada, lo que permite una actualización segura de vistas materializadas que no son de confianza. La víctima es un superusuario o miembro de uno de los roles del atacante. El ataque requiere atraer a la víctima para que ejecute ACTUALIZAR VISTA MATERIALIZADA CONCURRENTE en la vista materializada del atacante. Como parte de la explotación de esta vulnerabilidad, el atacante crea funciones que utilizan CREATE RULE para convertir la tabla temporal creada internamente en una vista.

A. Productos afectados:

- Versiones de PostgreSQL 12.x anteriores a 12.18.
- Versiones de PostgreSQL 13.x anteriores a 13.14.
- Versiones de PostgreSQL 14.x anteriores a 14.11.
- Versiones de PostgreSQL 15.x anteriores a 15.6.
- Versiones de PostgreSQL 16.x anteriores a 16.2.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad. Asimismo, para una defensa en profundidad. La versión 16.2 de PostgreSQL agrega las protecciones que utilizan las ramas más antiguas para corregir la vulnerabilidad.

Fuente de Información:	• hxxps://www.postgresql.org/about/news/postgresql-162-156-1411-1314-and-1218-released-2807/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°035	Fecha: 09-02-2024
		Página: 7 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en IBM Sterling Transformation Extender		
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 múltiples vulnerabilidades de severidad **ALTA** y **MEDIA** de tipo deserialización de datos que no son de confianza, validación de entrada incorrecta y fallo de segmentación en IBM Sterling Transformation Extender. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino, interrumpir el servicio, manipular datos y realizar un ataque de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2022-40609 de tipo deserialización de datos que no son de confianza, existe debido a una validación de entrada insegura al procesar datos serializados. Un atacante remoto puede pasar datos especialmente diseñados a la aplicación y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-22081 de tipo validación de entrada incorrecta, existe debido a una validación de entrada incorrecta dentro del componente JSSE en Oracle GraalVM para JDK. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para interrumpir el servicio.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-22067 de tipo validación de entrada incorrecta, existe debido a una validación de entrada incorrecta dentro del componente CORBA en Oracle Java SE. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para manipular datos.

Se ha asignado el siguiente identificador para la vulnerabilidad de severidad baja: CVE-2023-5676.

A. Productos afectados:

- IBM Sterling Transformation Extender: 10.1.0 - 11.0.0.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://www.ibm.com/support/pages/node/7116376

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°035**	**Fecha: 09-02-2024**
		Página: 8 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad alta en productos Qolsys		
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:

Cody Jung ha reportado una vulnerabilidad de severidad **ALTA** de tipo exposición de información sensible a un actor no autorizado en productos Qolsys. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto obtener información confidencial.

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-0242 de tipo exposición de información sensible a un actor no autorizado, podría permitir que el *software* de los productos afectados, bajo ciertas circunstancias, proporcionase acceso no autorizado a la configuración exponiendo información sensible al atacante. Esta vulnerabilidad, expone información confidencial a un actor que no está explícitamente autorizado a tener acceso a esa información.

A. Productos afectados:

Versiones anteriores a 4.4.2 de los productos:

- Qolsys IQ Panel 4.
- Qolsys IQ4 Hub.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión IQ Panel 4 e IQ4 Hub a la versión 4.4.2 (remota o manualmente, aplicando el parche iqpanel4.4.2*)*.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-039-01

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°035	Fecha: 09-02-2024
		Página: 9 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Suplantación de identidad de la plataforma de entretenimiento en línea Netflix		
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		

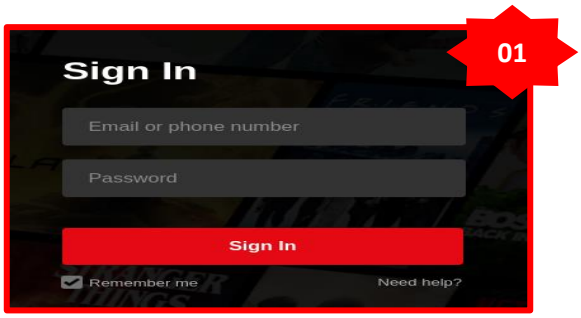
Descripción

1. **ANTECEDENTES:**

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que ciberdelincuentes vienen llevando a cabo una campaña de Phishing, quienes vienen suplantando la identidad de la empresa de entretenimiento y plataforma de Streaming Netflix, el supuesto sitio web cuenta con logos característicos al oficial, el cual tiene como finalidad robar sus credenciales de acceso y datos bancarios.

2. **DETALLES:**

El proceso del Phishing es el siguiente:



Paso N.º 01

Sitio web fraudulento de Netflix, solicita a la víctima registrar las credenciales de acceso (Correo electrónico y contraseña), para luego dar clic en <**Iniciar Sesión**>.

Paso N.º 02

Luego de darle clic en <Iniciar sesión>, solicita a la víctima que actualice su dirección de facturación como su nombre, dirección, ciudad, estado, teléfono y fecha de nacimiento para luego dar clic en <**Actualizar**>.

Paso N.º 03

Luego solicita que confirme el método de pago registrando su nombre, número de tarjeta, fecha de vencimiento y código de seguridad, para luego darle clic en <**confirmar forma de pago**>.

Paso N.º 04

Al completar con lo requerido y darle clic en iniciar sesión es redirigido al sitio web oficial de la plataforma de entretenimiento; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

A. Comparación del sitio web oficial y fraudulento.

- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento POSEE protocolo de seguridad de red (https), sin embargo, es malicioso.
- Existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

B. Proveedores de seguridad informática ALERTAN COMO SUPLANTACIÓN DE IDENTIDAD – PHISHING, 18 proveedores de seguridad marcaron este dominio como malicioso.

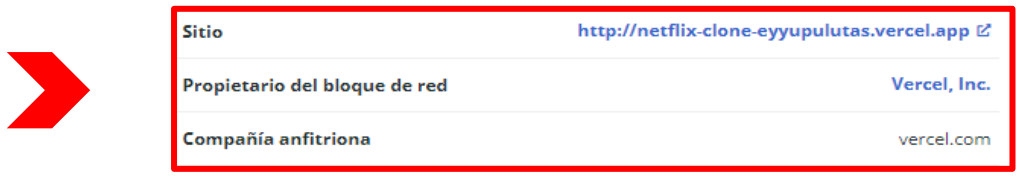
alfaMontaña.ai	Suplantación de identidad	Avira	Suplantación de identidad
BitDefender	Suplantación de identidad	Clúster25	Suplantación de identidad
CRDF	Malicioso	propiedad intelectual criminal	Suplantación de identidad
CyRadar	Malicioso	ESET	Suplantación de identidad
Buscador de amenazas Forcepoint	Suplantación de identidad	Datos G	Suplantación de identidad
Navegación segura de Google	Suplantación de identidad	Kaspersky	Suplantación de identidad
Ieonico	Suplantación de identidad	Base de datos de phishing	Suplantación de identidad
Sofos	Suplantación de identidad	Onda de confianza	Suplantación de identidad
VIPRE	Suplantación de identidad	raíz web	Malicioso

C. Indicadores de compromiso (IoC)

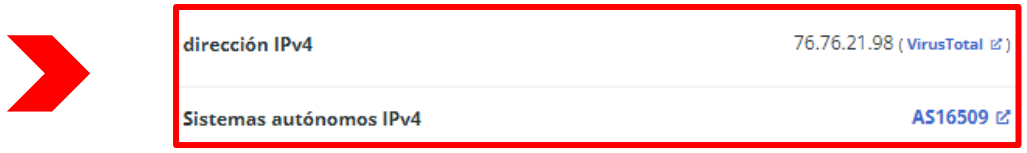
- Dominio : clon-netflix-eyyupulutas[.]vercel[.]app

Dominio	vercel.aplicación
Nombre del servidor	ns1.vercel-dns.com
registrador de dominio	nic.google

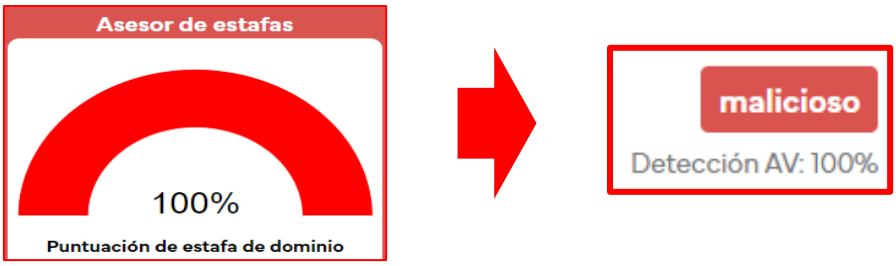
- URL : hxxp://netflix-clone-eyyupulutas[.]vercel[.]app



- IP : 76[.]76[.]21[.]98



- Servidor : AMAZON-02
- SHA-256 : 4276af3669a141a59388bc56a87f6614d9a9bdddf560636c264219a7eb11256f
- Tipo de tex. : Text/Html
- **Otras Detenciones**



D. Cómo funciona el Phishing:

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, Telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.).

E. Referencia:

Phishing o suplantación de identidad, es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- No aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.

Índice alfabético