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

025-2025-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°025	Fecha: 30-01-2025
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El malware Tria Stealer ataca dispositivos Android para recopilar datos SMS		
Tipo de Ataque	Stealers	Abreviatura	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:

Investigadores de ciberseguridad han descubierto una sofisticada campaña de malware para Android conocida como “Tria Stealer”, que intenta recopilar información confidencial como datos de SMS, registros de llamadas, mensajes de WhatsApp y correos electrónicos. Esta campaña utiliza invitaciones de boda como señuelo para engañar a las víctimas para que descarguen aplicaciones maliciosas.

2. DETALLES:

El malware Tria Stealer se hace pasar por una aplicación legítima de Android, que suele tener como tema las invitaciones de boda. Las víctimas son engañadas para que instalen la aplicación al recibir mensajes a través de WhatsApp o Telegram, a menudo enviados por cuentas comprometidas.

Una vez descargada e instalada, la aplicación solicita permisos peligrosos, como acceso a SMS, registros de llamadas y estado de la red. Luego recopila información como detalles del dispositivo, incluidos mensajes de aplicaciones como WhatsApp y Gmail. También se hace pasar por una aplicación de configuración del sistema para evitar sospechas.

Estos datos luego se filtran a los atacantes a través de bots de Telegram, que actúan como servidores de Comando y Control (C2).

El malware utiliza la función BroadcastReceiver para monitorear mensajes y llamadas entrantes, lo que le permite interceptar información crítica como contraseñas de un solo uso (OTP) y códigos de autorización de transacciones (TAC). Estos códigos se utilizan luego para secuestrar cuentas en plataformas como WhatsApp, Telegram y aplicaciones bancarias.

Además, las variantes más nuevas incluyen una funcionalidad para robar datos de notificaciones publicadas por aplicaciones de mensajería y correo electrónico populares, como Gmail, WhatsApp Business y Yahoo Mail.

Los datos robados se empaquetan nuevamente en formatos específicos y se envían a diferentes bots de Telegram según su tipo, lo que muestra un enfoque organizado por parte de los actores de la amenaza.

Luego que Tria Stealer compromete las cuentas, se propaga a los contactos de la víctima a través de chats grupales y mensajes directos, y termina solicitando transferencias de dinero a esos mismos contactos.

Los expertos advierten que la información robada también podría usarse para otros fines nefastos, como restablecer contraseñas de cuentas, acceder a sistemas bancarios en línea o comprometer plataformas adicionales que dependen de la autenticación por SMS o correo electrónico.

3. RECOMENDACIONES:

- Evitar descargar archivos APK de fuentes desconocidas, por el contrario, solo descargar aplicaciones directamente de fuentes confiables como Google Play Store.
- Verificar los mensajes que solicitan instalaciones de aplicaciones antes de hacer clic, incluso si parecen provenir de amigos o contactos de confianza.
- Habilitar la autenticación de dos factores (2FA) siempre que sea posible.
- Utilizar soluciones de seguridad confiables móviles para detectar y bloquear malware.

Fuente de Información:	• hxxps://gbhackers.com/tria-stealer-malware/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°025	Fecha: 30-01-2025 Página: 5 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en el software ISC BIND DNS		
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:

Internet Systems Consortium (ISC) ha publicado múltiples vulnerabilidades de severidad **ALTA** de tipo agotamiento de recursos que afectan a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto provocar el agotamiento de la CPU en servidores DNS autorizados y agotar los recursos del sistema bajo cargas de consultas pesadas.

2. DETALLES:

BIND 9, un software ampliamente utilizado para la resolución de nombres de dominio, desarrollado por el Internet Systems Consortium (ISC), BIND 9 es la implementación estándar de DNS para sistemas operativos tipo Unix, incluido Linux.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-11187 de tipo consumo excesivo de recursos del servidor en el software ISC BIND DNS, podría permitir a un atacante remoto provocar el agotamiento de la CPU en servidores DNS autorizados. La vulnerabilidad permite a un atacante crear consultas de zona DNS que generen respuestas que contengan una gran cantidad de registros en la sección adicional. Esto puede sobrecargar los recursos del servidor, lo que genera un alto uso de la CPU y potencialmente causar interrupciones del servicio para usuarios legítimos.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-12705 de tipo agotamiento de recursos que afecta al software ISC BIND, específicamente a su implementación DNS-over-HTTPS (DoH), podría permitir a un atacante remoto inundar un sistema de resolución de DNS con tráfico HTTP/2 diseñado, lo que puede provocar el agotamiento de la CPU y/o la memoria. La vulnerabilidad se puede explotar de forma remota sin ninguna autenticación, lo que hace que sea relativamente fácil para los atacantes iniciar un ataque. Debido a la naturaleza del ataque, en el que no se requiere autenticación para su explotación, los atacantes pueden iniciar fácilmente un ataque de denegación de servicio. Esto podría provocar la indisponibilidad total de los servicios DNS para los usuarios legítimos, lo que afectaría a los sitios web y las aplicaciones que dependen de la resolución DNS.

A. Productos afectados:

- Versión 9.11.0 hasta la 9.11.37.
- Versión 9.16.0 hasta la 9.16.50.
- Versión 9.18.0 hasta la 9.18.32.
- Versión 9.20.0 hasta la 9.20.4.
- Versión 9.21.0 hasta la 9.21.3.
- 9.11.3-S1 hasta 9.11.37-S1.
- 9.16.8-S1 hasta 9.16.50-S1.
- 9.18.11-S1 hasta el 9.18.32-S1.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan estas vulnerabilidades. La vulnerabilidad CVE-2024-11187 representa un riesgo para los servicios DNS que ejecutan versiones vulnerables de BIND 9, lo que requiere actualizaciones rápidas para mantener la integridad y la disponibilidad del servicio.
- Implementar una limitación de velocidad en las solicitudes entrantes y monitorear los patrones de tráfico puede ayudar a detectar y prevenir intentos de explotación antes de que se agraven.

Fuente de Información:	• hxxps://kb.isc.org/docs/cve-2024-11187 • hxxps://kb.isc.org/docs/cve-2024-12705

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°025	Fecha: 30-01-2025 Página: 6 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades de severidad alta que afecta al 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:

Se ha publicado múltiples vulnerabilidades de severidad **ALTA** de tipo escritura fuera de límites que afectan al marco eBPF (Extended Berkeley Packet Filter) del kernel de Linux. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante no autenticado obtener el control del kernel, ejecutar código arbitrario a nivel de kernel y escalar privilegios al nivel raíz.

2. DETALLES:

eBPF es una potente tecnología que permite que los programas se ejecuten en el espacio del kernel del sistema operativo de código abierto Linux.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-56614 de tipo desbordamiento de búfer en el kernel de Linux, específicamente en la función xsk_map_delete_elem del marco de sockets AF_XDP, podría permitir a un atacante remoto obtener el control del kernel, ejecutar código arbitrario y escalar privilegios al nivel raíz. La vulnerabilidad existe debido a un problema de desbordamiento de entero durante una comprobación de límites. En concreto, un entero sin signo que representa la cantidad máxima de entradas en un mapa se puede manipular para eludir las comprobaciones contra un entero con signo controlado por el usuario. Esto permite a un atacante utilizar valores negativos como índices de matriz, lo que provoca escrituras fuera de los límites y posible corrupción de la memoria.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-56615 de tipo escritura fuera de límites afecta al marco eBPF del kernel de Linux, particularmente dentro de la funcionalidad devmap_map_delete_elem durante la eliminación de elementos. Esta vulnerabilidad se caracteriza por una condición de escritura fuera de límites (OOB) que surge de un acceso incorrecto al índice debido a que el índice se define como un entero con signo. Esta configuración incorrecta puede provocar corrupción de memoria y un posible secuestro del flujo de control, lo que permite a los atacantes ejecutar código arbitrario con privilegios a nivel de kernel.

Se ha publicado código de explotación de prueba de concepto (PoC) para ambas vulnerabilidades, lo que aumenta significativamente la probabilidad de explotación activa.

A. Productos afectados:

- kernel de Linux, versión 4.14.
- kernel de Linux, versión 4.18.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Actualizar periódicamente con las últimas versiones del kernel.
- Mantenerse informado sobre nuevas vulnerabilidades y parches a través de canales oficiales como la lista de correo del kernel de Linux o avisos de seguridad de organizaciones confiables.

Fuente de Información:	• hxxps://git.kernel.org/stable/c/4d03f705e9d7aabebc6bfa5810f8aab6d176cbb7 • hxxps://git.kernel.org/stable/c/ed08c93d5a9801cc8f224a046411fd603c538d07 • hxxps://git.kernel.org/stable/c/f8abd03f83d5fe81e76eb93e2c4373eb9f75fd8a • hxxps://git.kernel.org/stable/c/d486b5741d987d3e0e6be4ac22cafdf94e6d1a47 • hxxps://git.kernel.org/stable/c/32cd3db7de97c0c7a018756ce66244342fd583f0

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°025	Fecha: 30-01-2025
		Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad de crítica en Microsoft Azure		
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 Corporation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo omisión de autenticación mediante la suplantación de identidad que afecta Azure AI Face Service. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante autorizado eludir la autenticación mediante técnicas de suplantación de identidad, lo que le permite elevar los privilegios en una red.

2. DETALLES:

Microsoft Azure es una plataforma integral de computación en la nube desarrollada por microsoft, diseñada para crear, probar, implementar y administrar aplicaciones y servicios a través de una red global de centros de datos.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-21415 de tipo omisión de autenticación mediante la suplantación de identidad Azure AI Face Service, podría permitir a un atacante autorizado eludir la autenticación mediante técnicas de suplantación de identidad, lo que le permite elevar los privilegios en una red. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante acceder a información sensible, realizar cambios no autorizados en sistemas críticos y bloquear el acceso a usuarios legítimos.

Las implicaciones de esta vulnerabilidad son significativas, ya que potencialmente puede permitir a los atacantes obtener acceso no autorizado a funcionalidades confidenciales dentro del Servicio Azure AI Face, lo que lleva a una mayor explotación y violaciones de datos.

Las organizaciones que utilizan este servicio deben priorizar la aplicación de cualquier parche o mitigación disponible tan pronto como se publiquen para protegerse contra posibles amenazas derivadas de esta vulnerabilidad.

A. Productos afectados:

- Azure AI Face Service, múltiples versiones.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Evaluar y ajustar las configuraciones de seguridad del servicio. Asegúrese de que las políticas de acceso y autenticación estén correctamente implementadas y sean lo más restrictivas posibles.
- Implementar autenticación multifactor para agregar una capa extra de seguridad que dificulte el acceso no autorizado, incluso si un atacante logra eludir la autenticación básica.
- Implementar mecanismos robustos de autenticación multifactor.
- Validar adecuadamente todas las credenciales y entradas del usuario.
- Monitorear y auditar accesos para detectar actividades sospechosas.
- Concientizar a los usuarios sobre las mejores prácticas en seguridad cibernética, incluyendo cómo reconocer intentos de phishing y otros métodos que podrían usarse para explotar esta vulnerabilidad.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21415

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°025	Fecha: 30-01-2025 Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades de severidad crítica en los dispositivos de la serie CPE de Zyxel		
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:

ZyXEL Communications Corp., ha publicado dos vulnerabilidades de severidad **CRÍTICA** de tipo inyección de comandos e inyección de comando del SO en los dispositivos de la serie CPE de Zyxel. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar comandos arbitrarios en el sistema objetivo, y con ello, resultar en el compromiso completo del sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-40891 de tipo inyección de comandos remotos en los dispositivos de la serie CPE de Zyxel, podría permitir a un atacante remoto no autenticado ejecutar comandos arbitrarios en el sistema objetivo. La vulnerabilidad existe debido a una validación de entrada incorrecta. Un atacante remoto no autenticado puede enviar paquetes especialmente diseñados a la interfaz Telnet de un dispositivo y ejecutar comandos arbitrarios del sistema operativo en el sistema de destino. Tener en cuenta que esta vulnerabilidad está siendo explotado activamente en la naturaleza.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-40890 de tipo inyección de comandos del SO en los dispositivos de la serie CPE de Zyxel, podría permitir a un atacante remoto ejecutar comandos de shell arbitrarios en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada incorrecta. Un atacante remoto no autenticado puede enviar una solicitud HTTP especialmente diseñada al dispositivo afectado y ejecutar comandos arbitrarios del sistema operativo en el sistema de destino.

A fines de enero de 2025, la empresa de ciberseguridad GreyNoise observó múltiples intentos de explotación activos dirigidos contra esta vulnerabilidad. Se informa que más de 1500 dispositivos vulnerables están expuestos en línea, principalmente ubicados en regiones como Filipinas, Turquía y partes de Europa.

A pesar de los posibles riesgos y los ataques en curso, Zyxel no ha emitido un aviso público ni un parche para esta vulnerabilidad. Los investigadores han detectado que los intentos de explotación se han vinculado a ciertas cepas de la botnet Mirai.

A. Productos afectados:

- Serie CPE de Zyxel: todas las versiones.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software cuando estén disponibles.
- Limitar el acceso únicamente a direcciones IP confiables a las interfaces administrativas de los dispositivos. Esto limita la exposición a posibles atacantes.
- Deshabilitar la administración remota si no es necesaria, para minimizar la exposición.
- Supervisar el tráfico para detectar solicitudes telnet inusuales dirigidas a las interfaces de administración de dispositivos Zyxel.
- Revisar periódicamente los canales oficiales de Zyxel para ver si hay anuncios sobre parches e impleméntelos tan pronto como estén disponibles.

Fuente de Información:	• hxxp://www.greynoise.io/blog/active-exploitation-of-zero-day-zyxel-cpe-vulnerability-cve-2024-40891 • hxxp://viz.greynoise.io/tags/zyxel-cpe-cve-2024-40890-command-injection-attempt

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°025	Fecha: 30-01-2025 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de desbordamiento de búfer basados en montón en VLC Media Player		
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:

La organización VideoLAN ha publicado una vulnerabilidad de severidad **ALTA** de tipo desbordamiento de búfer basados en montón en VLC Media Player. 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 **alta** identificada por MITRE como CVE-2024-46461 de tipo desbordamiento de búfer basado en montón en VLC Media Player, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino. El ataque requiere baja complejidad y pocos privilegios, pero necesita la interacción del usuario para una explotación exitosa.

La vulnerabilidad existe debido a un error de límite al manejar transmisiones MMS. Un atacante remoto puede engañar a la víctima para que se conecte a un servidor MMS malicioso, desencadenar un desbordamiento de búfer basado en el montón y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

A. Productos afectados:

- VLC Media Player: 3.0.0 - 3.0.20.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión 3.0.21 o superior que aborda esta vulnerabilidad.
- Implementar el monitoreo de actividades inusuales relacionadas con transmisiones de medios, especialmente aquellas que utilizan el protocolo MMS.
- Utilizar entornos aislados de aplicaciones y sistemas de detección de intrusiones basados en host (HIDS) para evitar intentos de explotación.
- Implementar reglas de firewall y segmentación de red adecuadas para limitar la exposición a transmisiones multimedia potencialmente maliciosas.
- Concientizar a los usuarios sobre los riesgos de abrir archivos multimedia desconocidos o sospechosos.

Fuente de Información:	• hxxps://www.videolan.org/security/sb-vlc3021.html

Índice alfabético