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

125-2024-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°125	Fecha: 29-05-2024 Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Aumento de los ataques de malware de Discord al descubrirse 50.000 enlaces maliciosos		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Los investigadores de ciberseguridad de Bitdefender han descubierto un aumento en los ataques de malware y phishing en Discord, observando 50.000 enlaces maliciosos en los últimos seis meses, siendo los usuarios estadounidenses los más atacados.

Estos hallazgos no deberían sorprender, ya que Discord tiene un historial de actividades maliciosas. En febrero del año pasado, se descubrió que los ciberdelincuentes explotaban la plataforma para difundir el malware PureCrypter, dirigido a organizaciones y entidades gubernamentales en América del Norte y la región de Asia y el Pacífico.

En julio de 2022, investigadores de ciberseguridad de Intel471 informaron que los ciberdelincuentes implementaron bots en Discord y Telegram para entregar malware capaz de robar credenciales de inicio de sesión de usuarios y datos financieros.

2. DETALLES:

En un análisis reciente de seis meses, la empresa de ciberseguridad Bitdefender ha descubierto una tendencia preocupante: los ciberdelincuentes están utilizando Discord, una popular plataforma de comunicación, para distribuir malware y ejecutar campañas de phishing.

El informe, compartido por Bitdefender, antes de su publicación el miércoles 29 de mayo del 2024, destaca más de 50.000 enlaces maliciosos identificados en Discord, lo que muestra la creciente vulnerabilidad de la plataforma a las amenazas cibernéticas.

Los enlaces de malware y phishing representan en conjunto el 39% de los enlaces maliciosos detectados. Estos ataques a menudo implican tácticas engañosas para engañar a los usuarios para que descarguen software dañino o proporcionen información confidencial.

Los usuarios de Estados Unidos están particularmente en riesgo, ya que representan el 16,2 % de las amenazas. Esto los convierte en el grupo más objetivo por un margen significativo. Otros países objetivo de campañas maliciosas a través de Discord incluyen Francia, Rumania, el Reino Unido y Alemania.

Una estafa común implica ofertas falsas de Discord Nitro gratuito, un servicio de suscripción premium. Los usuarios se sienten atraídos por la promesa de actualizaciones gratuitas, sólo para ser blanco de ataques de phishing o malware.

3. RECOMENDACIONES:

- Tener cuidado con las ofertas gratuitas, con los enlaces o mensajes que ofrecen Discord Nitro gratis u otras ofertas sospechosas. Verificar dichas ofertas a través de canales oficiales.
- Habilitar la autenticación de dos factores. Esto agrega una capa adicional de seguridad a su cuenta de Discord, lo que dificulta el acceso de los atacantes.
- Utilizar software antivirus, actualizarlo y ejecutarlo periódicamente para detectar y eliminar posibles amenazas.
- Informar alguna actividad sospechosa. Si encuentra un enlace o mensaje sospechoso, infórmelo al equipo de soporte de Discord para ayudar a proteger a la comunidad.

Fuente de Información:	• hxxps://hackread.com/discord-malware-attacks-as-50000-malicious-links/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°125	Fecha: 29-05-2024 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica de ejecución remota de código en servidor Managed File Transfer Platform Server de TIBCO		
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 escalada de privilegios del servidor TIBCO Managed File Transfer Platform para Unix y z/Linux. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto omitir la autenticación de ID de usuario/contraseña y transferir archivos como root o incluso ejecutar comandos como root.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-4407 de tipo escalada de privilegios podría permitir a un atacante remoto eludir la autenticación de usuario/contraseña y transferir archivos o ejecutar comandos como super usuario.

La explotación exitosa de esta vulnerabilidad incluye la posibilidad teórica de permitir a los clientes de Platform Server omitir la autenticación de ID de usuario/contraseña y transferir archivos como root o incluso ejecutar comandos como root. Para que ocurra este problema, la configuración del producto debe desviarse de los estándares de configuración sugeridos de Platform Server. Este problema sólo ocurre cuando Platform Server se inicia como root; Cuando Platform Server se inicia como no raíz, los archivos no se pueden transferir como raíz y los comandos no se pueden ejecutar como raíz.

A. Productos afectados:

- Servidor TIBCO Managed File Transfer Platform para Unix versiones 8.0.0, 8.0.1, 8.1.0, 8.1.1.
- Servidor TIBCO Managed File Transfer Platform para z/Linux versiones 8.0.0, 8.0.1, 8.1.0, 8.1.1.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión 8.0.2 o 8.1.2 (en Unix y z/Linux) que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://community.tibco.com/advisories/tibco-security-advisory-may-28-2024-tibco-managed-file-transfer-platform-server-for-unix-cve-2024-4407-r214/ • hxxps://community.tibco.com/advisories/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°125	Fecha: 29-05-2024 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en el sistema de archivos de formato de disco universal (UDF) en macOS		
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 desbordamiento de pila que afecta al sistema de archivos de formato de disco universal (UDF) en el sistema operativo macOS Sonoma de Apple. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto escalar privilegios y ejecutar código arbitrario con privilegios del kernel.

2. DETALLES:

MacOS Sonoma es la vigésima versión principal de macOS, el sistema operativo de escritorio de Apple para ordenadores Mac. macOS Sonoma admite varios modelos de Mac, incluidos MacBook Pro, MacBook Air, iMac, iMac Pro, Mac mini, Mac Studio y Mac Pro, con compatibilidad a partir de años específicos para cada dispositivo.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-27842 en el sistema de archivos de UDF en macOS, podría permitir a un atacante remoto escalar privilegios y ejecutar código arbitrario con privilegios del kernel. Esta vulnerabilidad se combina con funciones IOCTL (control de entrada y salida), que ejecutarán código arbitrario con privilegios del kernel.

Cyber Security News, publicó la prueba de concepto (PoC) de esta vulnerabilidad que menciona que esta vulnerabilidad existe en el componente IOAESAccelerator de macOS que se invoca. El código PoC utiliza cualquier aplicación para crear un búfer de longitud 0x28 bytes que se escribe en el búfer de pila de longitud 0x18 bytes. Esto crea una condición de desbordamiento de pila en el dispositivo afectado, lo que provoca un pánico en el kernel.

Además, combinar esta vulnerabilidad con los comandos ioctl aumentará la superficie de ataque que se puede escalar para ejecutar comandos sin restricciones en el dispositivo.

A. Productos afectados:

- MacOS Sonoma, versiones inferiores a 14.5.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión 14.5 que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://support.apple.com/en-us/HT214106

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°125	Fecha: 29-05-2024 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de divulgación de información de Check Point VPN		
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 violación de la protección SSL en Check Point VPN. 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-2024-24919 de tipo violación de la protección SSL en Check Point VPN, podría permitir a un atacante remoto obtener información confidencial. Esta vulnerabilidad permite a los atacantes leer cierta información confidencial una vez que están conectados a Internet. La vulnerabilidad se puede explotar sin requerir interacción del usuario ni privilegios especiales, lo que la hace particularmente preocupante.

Check Point indicó, que la vulnerabilidad permite a un atacante leer cierta información en puertas de enlace conectadas a Internet con acceso remoto VPN o acceso móvil habilitado. Igualmente, han observado la explotación de CVE-2024-24919 en la naturaleza, y los atacantes lo utilizan para extraer datos confidenciales de sistemas comprometidos y escalar privilegios dentro de las redes.

A. Productos afectados:

- Check Point CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways, Quantum Spark Appliances: Versión R77.20 (EOL), R77.30 (EOL), R80.10 (EOL), R80.20 (EOL), R80.20.x, R80.20SP (EOL), R80.30 (EOL), R80.30SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x y R81.20.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad.
- Cambiar la contraseña de la cuenta de Security Gateway en Active Directory si está configurado para utilizar una unidad de cuenta LDAP.
- Evitar que las cuentas locales se conecten a una VPN con autenticación de contraseña, se recomienda no utilizar cuentas locales que autentiquen a los usuarios de acceso remoto con autenticación de solo contraseña.
- Activar la protección que detecta los intentos de explotación de esta vulnerabilidad. Para que se active la protección, se debe actualizar el producto Security Gateway a la última actualización de IPS.
- Hacer clic en Protecciones, en la Puerta de enlace de seguridad R81 / R80 / R77 / R75, en la pestaña IPS, y buscar la protección de divulgación de información de Check Point VPN (CVE-2024-24919) utilizando la herramienta de búsqueda, y editar la configuración de protección e instalar la política en todos los Security Gateways.

Fuente de Información:	• hxxps://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0353.html • hxxps://support.checkpoint.com/results/sk/sk182336

Índice alfabético