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

131-2024-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°131	Fecha: 05-06-2024
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Zero-Day en TikTok permite secuestro de cuentas		
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:**

Durante la semana pasada, la popular plataforma para compartir vídeos TikTok reconoció un problema de seguridad que ha sido aprovechado por actores de amenazas para tomar el control de cuentas de alto perfil, pertenecientes a múltiples empresas y celebridades, como Paris Hilton, Sony y CNN, explotando una vulnerabilidad de día cero en la función de mensajes directos de las redes sociales.

El desarrollo fue informado por primera vez por Semafor y Forbes, que detallaron esta campaña de apropiación de cuentas, la cual permite que el malware propagado a través de mensajes directos comprometa cuentas sin tener que hacer clic o interactuar con ellas.

Esta no es la primera vez que se descubren problemas de seguridad en el servicio ampliamente utilizado. En enero de 2021, Check Point detalló una falla en TikTok que podría haber permitido a un atacante crear una base de datos de los usuarios de la aplicación y sus números de teléfono asociados para futuras actividades maliciosas.

Luego, en septiembre de 2022, Microsoft descubrió un exploit de un solo clic que afectaba a la aplicación de Android de TikTok y que podía permitir a los atacantes hacerse cargo de las cuentas cuando las víctimas hacían clic en un enlace especialmente diseñado.

Otro problema revelado por Imperva hace más de un año podría haber permitido a los atacantes monitorear la actividad de los usuarios y acceder a información confidencial tanto en dispositivos móviles como de escritorio.

2. **DETALLES:**

Si bien los detalles específicos sobre la naturaleza del ataque son escasos por el momento, VXUnderground explicó en su publicación en X (anteriormente Twitter) que un actor de amenazas desconocido descubrió un exploit en TikTok que permite a los usuarios secuestrar cuentas.

Se ha descubierto que el exploit aprovecha una vulnerabilidad de día cero en el componente de mensajería que permite ejecutar código malicioso tan pronto como se abre el mensaje. Es decir, la carga útil se entrega a través de mensajes directos de TikTok y se ejecuta cuando se lee, sin requerir archivos externos ni respuesta del usuario.

Tras verse comprometidas, dichas cuentas, se eliminaron de la plataforma para así evitar abusos. Las autoridades en estos momentos advierten que las cuentas hackeadas publican anuncios de trabajo y otras ofertas para el fraude de criptomonedas.

En la actualidad la empresa enfrenta una situación compleja en los Estados Unidos, esto debido a sospechas sobre el uso de la aplicación por parte del gobierno de China para espiar a ciudadanos norteamericanos, lo que impulsó una legislación que obliga a la empresa que gestiona la aplicación, ByteDance, para que se deshaga de ésta.

3. **RECOMENDACIÓN:**

- Actualizar Tiktok cuando lance la última versión para abordar esta vulnerabilidad.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2024/06/zero-day-en-tiktok-permite-secuestro-de.html • hxxps://hackread.com/tiktok-accounts-hacked-via-zero-click-attack-dm/ • hxxps://thehackernews.com/2024/06/celebrity-tiktok-accounts-compromised.html • hxxps://www.softzone.es/noticias/seguridad/tiktok-corrige-fallo-hackear-cuenta/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°131	Fecha: 05-06-2024 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en Cisco Finesse		
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 **MEDIA** de tipo falsificación de solicitud del lado del servidor (SSRF) que en la interfaz de administración basada en web de Cisco Finesse. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado llevar a cabo un ataque de falsificación de solicitud del lado del servidor (SSRF) y un ataque de secuencias de comandos entre sitios (XSS) almacenado explotando una vulnerabilidad RFI.

2. DETALLES:

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-20404 de tipo SSRF en la interfaz de administración basada en web de Cisco Finesse, podría permitir que un atacante remoto no autenticado lleve a cabo un ataque SSRF en un sistema afectado. Esta vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario para solicitudes HTTP específicas que se envían a un sistema afectado. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP diseñada al dispositivo afectado. Un exploit exitoso podría permitir al atacante obtener información confidencial limitada para los servicios asociados al dispositivo afectado.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-20405 de tipo XSS en la interfaz de administración basada en web de Cisco Finesse, podría permitir que un atacante remoto no autenticado lleve a cabo un ataque XSS almacenado explotando una vulnerabilidad RFI. Esta vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario para solicitudes HTTP específicas que se envían a un dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario para que haga clic en un enlace manipulado. Un exploit exitoso podría permitir al atacante ejecutar código de script arbitrario en el contexto de la interfaz afectada o acceder a información confidencial en el dispositivo afectado.

Las vulnerabilidades no dependen unas de otras. No es necesario explotar una de las vulnerabilidades para explotar la otra vulnerabilidad. Además, una versión de software que se ve afectada por una de las vulnerabilidades puede no verse afectada por la otra vulnerabilidad.

A. Productos afectados:

Estas vulnerabilidades afectan a Cisco Finesse (versión 11.6(1) ES11 y anteriores y 12.6(2) ES01 y anteriores) en la configuración predeterminada. Asimismo, los siguientes productos de Cisco que pueden estar incluidos con Cisco Finesse también se ven afectados por estas vulnerabilidades:

- Packaged Contact Center Enterprise (Packaged CCE).
- Unified Contact Center Enterprise (Unified CCE).
- Unified Contact Center Express (Unified CCX).
- Unified Intelligence Center.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-ssrf-rfi-Um7wT8Ew

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°131	Fecha: 05-06-2024 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en GStreamer		
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 Desbordamiento de búfer basado en pila en GStreamer. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

GStreamer es un framework multimedia de código abierto que se utiliza para crear aplicaciones multimedia, como streaming, reproducción multimedia, edición no lineal, y otros procesos de audio y vídeo. GStreamer es conocido por su arquitectura de complementos y librerías, lo que facilita el desarrollo de aplicaciones multimedia. Está disponible para una amplia variedad de sistemas operativos y procesadores, incluyendo Linux, Android, Windows, macOS, iOS, x86, ARM, MIPS, SPARC y otros.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-0444 de tipo desbordamiento de búfer basado en pila, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un error de límite al analizar archivos de vídeo codificados con AV1. Un atacante remoto puede engañar a la víctima para que abra un archivo de vídeo especialmente diseñado, provocar un desbordamiento de búfer basado en pila y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso total del sistema vulnerable.

A. Productos afectados:

- GStreamer: todas las versiones.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.zerodayinitiative.com/advisories/ZDI-24-567/ • hxxps://gitlab.freedesktop.org/gstreamer/gstreamer/-/commit/f368d63ecd89e01fd2cf0b1c4def5fc782b2c390

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°131	Fecha: 05-06-2024 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el Sistema de gestión de red ProSAFE de NETGEAR		
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 transversal de directorio en Sistema de gestión de red ProSAFE de NETGEAR. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en un dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-5505 en instalaciones afectadas de "NETGEAR ProSAFE Network Management System", podría permitir a un atacante remoto la ejecución remota de código arbitrario. Se requiere autenticación para aprovechar esta vulnerabilidad.

La vulnerabilidad existe dentro de la clase UpLoadServlet. El problema se debe a la falta de validación adecuada de una ruta proporcionada por el usuario antes de usarla en operaciones de archivos. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto de SYSTEM.

A. Productos afectados:

- NETGEAR ProSAFE Network Management System.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.zerodayinitiative.com/advisories/ZDI-24-563/ • hxxps://kb.netgear.com/000066192/Security-Advisory-for-Missing-Function-Level-Access-Control-on-the-NMS300-PSV-2024-0008

Índice alfabético