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

171-2024-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°171	Fecha: 24-07-2024 Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Los piratas informáticos abusan de Google Cloud para realizar phishing		
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:

Los piratas informáticos utilizan plataformas de todo tipo para lanzar sus ataques y campañas maliciosas. Pueden hacer uso de redes sociales, del correo electrónico o de la nube, entre otros muchos. En este caso, están utilizando la nube de Google para realizar ataques Phishing.

Google Cloud es el objetivo debido a sus amplios y potentes recursos, que podrían utilizarse para una multitud de actividades maliciosas.

La enorme cantidad de datos y la capacidad de procesamiento que ofrecen los servicios de Google Cloud suelen atraer a los actores maliciosos. Debido a la complejidad de los entornos de la nube, esto también puede permitirles pasar desapercibidos.

2. DETALLES:

Google Cloud Threat Horizons reveló recientemente que los piratas informáticos han estado abusando activamente de Google Cloud para realizar phishing.

El informe Google Cloud Threat Horizons, elaborado por varios equipos de Google, como TAG y Mandiant, revela inteligencia estratégica sobre amenazas a la seguridad de la nube entre proveedores.

Los profesionales de seguridad en la nube deben tener en cuenta tres áreas clave a la hora de desarrollar estrategias para abordar las amenazas emergentes de la nube sin servidor. Estas incluyen la mitigación de los riesgos derivados de las configuraciones incorrectas de los clientes y el aprovechamiento de la capacidad de expansión y la reducción de los costos operativos.

Las consideraciones que deben priorizarse son:

Credenciales comprometidas. Las contraseñas débiles o inexistentes siguen siendo la principal vía de entrada ilícita.

Configuración incorrecta explotada. Las configuraciones erróneas afectan a más del 30% de los casos y en su mayoría involucran claves de cuentas de servicio gratuitas.

Distribución de malware. Los cibercriminales, podrían distribuir de forma masiva software malicioso de todo tipo. Pueden ser keyloggers, ransomware, spyware, etc.

3. RECOMENDACIONES:

- Administrar estrictamente las cuentas con altos privilegios. Aplicar el principio del mínimo privilegio en las demás cuentas.
- Implementar controles de detección de malware. Colaborar con CISA para el análisis de malware. Utilizar la detección de amenazas de contenedores. Evitar los contenedores que no sean de confianza. Configurar los ajustes de red de Cloud Functions. Controlar el ingreso y egreso de la red para Cloud Run.
- Tener el equipo actualizado. Asegurarse de usar siempre las últimas versiones, ya sea del sistema operativo o de cualquier otro programa que tengas instalado.

Fuente de Información:	• hxxps://gbhackers.com/hackers-abusing-google-cloud/ • hxxps://www.redeszone.net/noticias/seguridad/nube-google-robo-contrasenas/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°171	Fecha: 24-07-2024
		Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en productos de la serie AFS/AFR de Hitachi Energy		
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** de tipo confusión de tipos, uso después de liberación, doble liberación y discrepancia observable que afecta a diversos productos de la serie AFS/AFR de Hitachi Energy. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto generar una condición de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-0286 de tipo confusión de tipos relacionada con el procesamiento de direcciones X.400 dentro de un GeneralName X.509. Las direcciones X.400 se analizaron como ASN1_STRING, pero la definición de estructura pública para GENERAL_NAME especificó incorrectamente el tipo del campo x400Address como ASN1_TYPE.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2022-0215 de tipo uso después de liberar en la función API pública BIO_new_NDEF es una función auxiliar que se utiliza para transmitir datos ASN.1 a través de una BIO. Se utiliza principalmente de forma interna en OpenSSL para admitir las capacidades de transmisión de SMIME, CMS y PKCS7, pero las aplicaciones de usuario final también pueden llamarla directamente.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-4450 de tipo doble libre en la función PEM_read_bio_ex() lee un archivo PEM de un BIO y analiza y decodifica el "nombre" (por ejemplo, "CERTIFICADO"), cualquier dato de encabezado y los datos de carga útil. Si la función tiene éxito, los argumentos "name_out", "header" y "data" se completan con punteros a los búferes que contienen los datos decodificados relevantes.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2022-4304 de tipo discrepancia observable, de debe a que existe un canal lateral basado en tiempo en la implementación de descifrado RSA de OpenSSL que podría ser suficiente para recuperar un texto simple a través de una red en un ataque de estilo Bleichenbacher. Para lograr un descifrado exitoso, un atacante tendría que poder enviar una gran cantidad de mensajes de prueba para el descifrado. La vulnerabilidad afecta a todos los modos de relleno RSA: PKCS#1 v1.5, RSA-OEAP y RSASVE.

A. Productos afectados:

- AFS650: Versión 9.1.08 y anteriores.
- AFS660-C: Versión 7.1.05 y anteriores.
- AFS665-B: Versión 7.1.05 y anteriores.
- AFS670-V2: Versión 7.1.05 y anteriores.
- AFS670: Versión 9.1.08 y anteriores.
- AFS675: Versión 9.1.08 y anteriores.
- AFS677: Versión 9.1.08 y anteriores.
- AFR677: Versión 9.1.08 y anteriores.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de firmware disponible que aborda estas vulnerabilidades.
- Actualizar el firmware del AFS 650 a la versión 9.1.10.
- Actualizar los productos AFS660-C, AFS665-B, AFS670-V2 a la versión de firmware 7.1.08 de AFS 66x.
- Actualizar los productos AFS670/675/677, AFR677 a la versión de firmware 9.1.10 de AFS/AFR 67x.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-205-02

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°171	Fecha: 24-07-2024
		Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en la aplicación de mensajería GroupMe de Microsoft		
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 control de acceso inadecuado en la aplicación gratuita de mensajería grupal "GroupMe" de Microsoft. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante no autenticado aumentar sus privilegios engañando a los usuarios para que hagan clic en enlaces maliciosos. Esto podría generar acceso no autorizado a información confidencial dentro de la aplicación GroupMe.

2. DETALLES:

GroupMe es una App mensajería instantánea para smartphones de Microsoft. La aplicación utiliza la red de datos del dispositivo móvil en el que se esté ejecutando, por lo tanto, funciona conectada a internet a diferencia de los servicios tradicionales de mensajes cortos o multimedia.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-38164 de tipo control de acceso inadecuado en GroupMe, podría permitir a un atacante obtener privilegios elevados en una red. El ataque generalmente requiere que se engañe a la víctima para que haga clic en un enlace malicioso o interactúe con un elemento comprometido dentro de la aplicación, lo que puede derivar en acceso no autorizado a información confidencial, modificación de datos e interrupción de servicios. El alcance se modifica, lo que indica que la vulnerabilidad afecta a recursos que van más allá de su alcance de seguridad.

La vulnerabilidad tiene un alto impacto en la confidencialidad y la integridad, lo que significa que los atacantes podrían potencialmente modificar o robar datos confidenciales de los usuarios. Asimismo, un atacante podría interrumpir los servicios, afectando el acceso de los usuarios y la funcionalidad dentro de GroupMe.

A. Productos afectados:

- GroupMe.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Aplicar el parche oficial publicado por Microsoft lo antes posible.
- Concientizar a los usuarios sobre los riesgos de hacer clic en enlaces desconocidos o sospechosos.
- Implementar la segmentación de la red para limitar la posible propagación si se explota la vulnerabilidad.
- Utilizar el principio del mínimo privilegio para minimizar el impacto de los ataques exitosos.
- Supervisar la actividad inusual o las escaladas de privilegios no autorizadas en la aplicación GroupMe.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38164 • hxxps://www.security-database.com/detail.php?alert=CVE-2024-38164&utm_source=feedly

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°171	Fecha: 24-07-2024 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de día cero en Telegram para Android		
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:

Investigadores de ESET han descubierto un exploit de día cero en la aplicación de Telegram para Android que permite enviar archivos maliciosos disfrazados de videos. La vulnerabilidad de severidad **CRÍTICA** de tipo validación de entrada incorrecta afecta a la aplicación Telegram para Android. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante distribuir aplicaciones maliciosas camufladas como archivos de vídeo a través de la aplicación Telegram para Android.

2. DETALLES:

La vulnerabilidad conocida como "EvilVideo" permite enviar aplicaciones maliciosas camufladas en videos en la aplicación Telegram para Android que afecta a las versiones 10.14.4 y anteriores. Esta vulnerabilidad está relacionada con una validación de entrada incorrecta. Al usar el exploit para explotar la vulnerabilidad "EvilVideo", los atacantes podrían compartir cargas útiles maliciosas de Android a través de canales, grupos y chat de Telegram, y hacer que aparezcan como archivos multimedia.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-7014 de tipo validación de entrada incorrecta, podría permitir a los atacantes distribuir aplicaciones maliciosas camufladas como archivos de vídeo a través de la aplicación Telegram para Android. Los usuarios podrían instalar estas aplicaciones maliciosas sin saberlo, lo que podría provocar acceso no autorizado, robo de datos o vulneración del dispositivo. El impacto es significativo dada la gran base de usuarios de Telegram y la confianza que estos depositan en el contenido compartido a través de la plataforma.

A. Productos afectados:

- Telegram para Android, todas las versiones hasta la 10.14.4.

B. Indicadores de compromiso:

- SHA-1: f159886dcf9021f41eaa2b0641a758c4f0c4033d.
- SHA-256: ef5b77c003be850406ff8a18a35eb094632dcdc8f6112efcde036e3c454dde0c.
- MD5: 19e5c726ccf1b1797cc6b379cf5ba41a.
- IP: 183.83.172[.]232.
- DOMINIO C2: infinityhackscharan.ddns[.]net.

3. RECOMENDACIONES:

- Actualizar el producto afectado Telegram para Android a la versión 10.14.5 que aborda esta vulnerabilidad.
- Concientizar a los usuarios sobre los riesgos de abrir o instalar cualquier archivo, incluso los que aparecen como videos, de fuentes no confiables.
- Implementar soluciones de administración de dispositivos móviles (MDM) para garantizar que todos los dispositivos de la empresa estén ejecutando la última versión parcheada de Telegram.
- Considerar el uso de listas blancas de aplicaciones para evitar la instalación de aplicaciones no autorizadas en los dispositivos de la empresa.
- Analizar regularmente los dispositivos en busca de malware y aplicaciones sospechosas.
- Monitorear cualquier actividad inusual o instalaciones no autorizadas en dispositivos con Telegram instalado.

Fuente de Información:	• hxxps://www.welivesecurity.com/en/eset-research/cursed-tapes-exploiting-evilvideo-vulnerability-telegram-android/

Índice alfabético