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, 01 de abril de 2024

076-2024-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°076	Fecha: 01-04-2024
		Página: 4 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	El malware bancario Vultur para Android se hace pasar por la aplicación McAfee Security		
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 seguridad encontraron una nueva versión del troyano bancario Vultur para Android que incluye capacidades de control remoto más avanzadas y un mecanismo de evasión mejorado.

Los investigadores de la empresa de detección de fraude ThreatFabric documentaron por primera vez el malware en marzo de 2021 y, a finales de 2022, observaron que se distribuía en Google Play a través de aplicaciones de cuentagotas.

A finales de 2023, la plataforma de seguridad móvil Zimperium incluyó a Vultur entre sus 10 troyanos bancarios más activos del año, señalando que nueve de sus variantes apuntaban a 122 aplicaciones bancarias en 15 países.

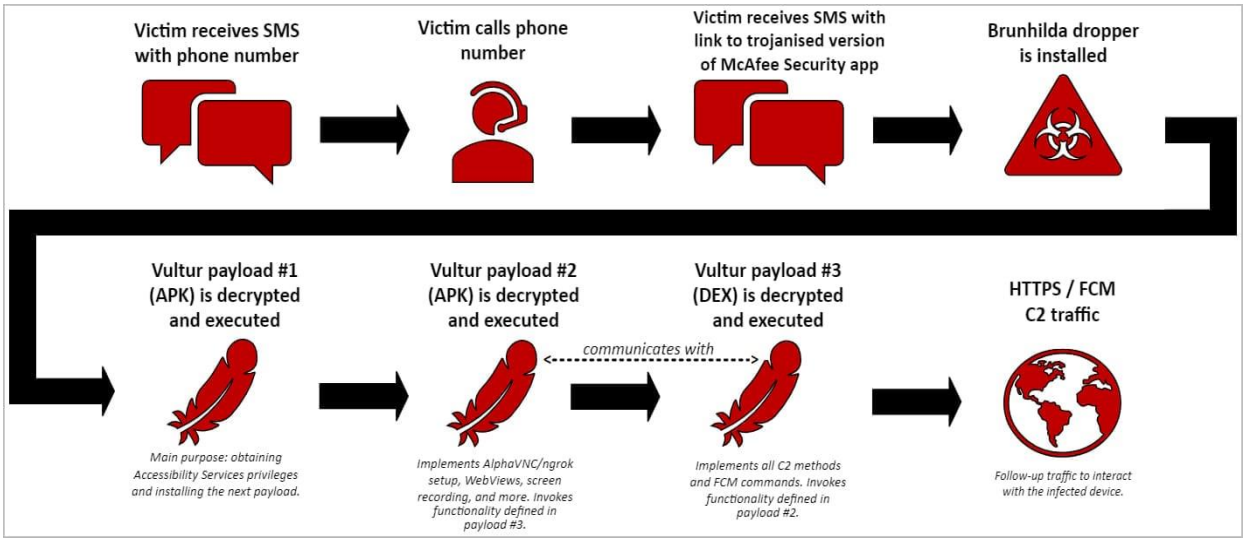
Un informe de Fox-IT, parte del Grupo NCC, advierte que una versión nueva y más evasiva de Vultur se propaga a las víctimas a través de un ataque híbrido que se basa en smishing (SMS phishing) y llamadas telefónicas que engañan a los objetivos para que instalen una versión del malware que se hace pasar por la aplicación McAfee Security.

2. DETALLES:

La última cadena de infección de Vultur comienza cuando la víctima recibe un mensaje SMS alertando de una transacción no autorizada y le indica que llame a un número proporcionado para obtener orientación.

La llamada es respondida por un estafador que persuade a la víctima para que abra el enlace que llega con un segundo SMS, que dirige a un sitio que ofrece una versión modificada de la aplicación McAfee Security.

Dentro de la aplicación troyanizada McAfee Security se encuentra el dropper de malware 'Brunhilda'.



Tras la instalación, la aplicación descifra y ejecuta tres cargas útiles relacionadas con Vultur (dos APK y un archivo DEX) que obtienen acceso a los Servicios de Accesibilidad, inicializan los sistemas de control remoto y establecen una conexión con el servidor de comando y control (C2).

La última versión del malware Vultur que analizaron los investigadores mantiene varias características clave de iteraciones anteriores, como grabación de pantalla, registro de teclas y acceso remoto a través de AlphaVNC y ngrok, lo que permite a los atacantes monitoreo y control en tiempo real.

En comparación con las variantes anteriores, el nuevo Vultur ha introducido una serie de características nuevas, que incluyen:

- Acciones de administración de archivos que incluyen descargar, cargar, eliminar, instalar y buscar archivos en el dispositivo.
- Uso de Servicios de Accesibilidad para realizar clics, desplazamientos y gestos de deslizamiento.
- Bloquear aplicaciones específicas para que no se ejecuten en el dispositivo, y mostrar HTML personalizado o un mensaje de "No disponible temporalmente" al usuario.
- Mostrar notificaciones personalizadas en la barra de estado para engañar a la víctima.
- Desactivar Keyguard para evitar la seguridad de la pantalla de bloqueo y obtener acceso sin restricciones al dispositivo.

Además de estas características, la última versión de Vultur también ha agregado nuevos mecanismos de evasión, como cifrar sus comunicaciones C2 (AES + Base64), utilizar múltiples cargas útiles cifradas que se descifran sobre la marcha cuando es necesario y enmascarar sus actividades maliciosas bajo la apariencia de aplicaciones legítimas.

Además, el malware utiliza código nativo para descifrar la carga útil, lo que dificulta el proceso de ingeniería inversa y también ayuda a evadir la detección.

IOCs:

Hash (SHA-256):

- edef007f1ca60fdf75a7d5c5ffe09f1fc3fb560153633ec18c5ddb46cc75ea21 - Brunhilda Dropper.
- 89625cf2caed9028b41121c4589d9e35fa7981a2381aa293d4979b36cf5c8ff2 - Vultur payload #1.
- 1fc81b03703d64339d1417a079720bf0480fece3d017c303d88d18c70c7aabc3 - Vultur payload #2.
- 4fed4a42aadea8b3e937856318f9fbd056e2f46c19a6316df0660921dd5ba6c5 - Vultur payload #3.
- 001fd4af41df8883957c515703e9b6b08e36fde3fd1d127b283ee75a32d575fc - Brunhilda Dropper.
- fc8c69bddd40a24d6d28fbf0c0d43a1a57067b19e6c3cc07e2664ef4879c221b - Vultur payload #1.
- 7337a79d832a57531b20b09c2fc17b4257a6d4e93fcaeb961eb7c6a95b071a06 - Vultur payload #2.
- 7f1a344d8141e75c69a3c5cf61197f1d4b5038053fd777a68589ecdb29168e0c - Vultur payload #3.
- 26f9e19c2a82d2ed4d940c2ec535ff2aba8583ae3867502899a7790fe3628400 - Brunhilda Dropper.
- 2a97ed20f1ae2ea5ef2b162d61279b2f9b68eba7cf27920e2a82a115fd68e31f - Vultur payload #1.
- c0f3cb3d837d39aa3abccada0b4ecdb840621a8539519c104b27e2a646d7d50d - Vultur payload #2.
- 92af567452ecd02e48a2ebc762a318ce526ab28e192e89407cac9df3c317e78d - Brunhilda Dropper.
- fa6111216966a98561a2af9e4ac97db036bcd551635be5b230995faad40b7607 - Vultur payload #1.
- dc4f24f07d99e4e34d1f50de0535f88ea52cc62bfb520452bdd730b94d6d8c0e - Vultur payload #2.
- 627529bb010b98511cfa1ad1aaa08760b158f4733e2bbccfd54050838c7b7fa3 - Vultur payload #3.
- f5ce27a49eaf59292f11af07851383e7d721a4d60019f3aceb8ca914259056af - Brunhilda Dropper.
- 5d86c9afd1d33e4affa9ba61225aded26ecaeb01755eeb861bb4db9bbb39191c - Vultur payload #1.
- 5724589c46f3e469dc9f048e1e2601b8d7d1bafcc54e3d9460bc0adeeada022d - Vultur payload #2.
- 7f1a344d8141e75c69a3c5cf61197f1d4b5038053fd777a68589ecdb29168e0c - Vultur payload #3.
- fd3b36455e58ba3531e8cce0326cce782723cc5d1cc0998b775e07e6c2622160 - Brunhilda Dropper.

3. RECOMENDACIONES:

- Descargar aplicaciones exclusivamente de fuentes oficiales como Google Play.
- Verificar los permisos que solicita una aplicación cuando se instala y asegurarse de otorgar su consentimiento solo a aquellos necesarios para la funcionalidad principal de la aplicación.
- Verificar la fuente de información de tus correos entrantes.
- Implementar soluciones de seguridad integrales que puedan detectar y bloquear malware.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/vultur-banking-malware-for-android-poses-as-mcafee-security-app/#google_vignette • hxxps://cultura-informatica.com/android/malware-vultur-para-android/ • hxxps://research.nccgroup.com/2024/03/28/android-malware-vultur-expands-its-wingspan/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°076	Fecha: 01-04-2024
		Página: 6 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en la librería XZ Utils		
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:

Andres Freund, ingeniero de *software* de Microsoft ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo código malicioso integrado (puerta trasera) en XZ Utils. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto obtener acceso no autorizado a la aplicación.

2. DETALLES:

XZ Utils es una colección de programas para comprimir y descomprimir archivos usando el formato de compresión LZMA/LZMA2. Este formato es conocido por ofrecer altas tasas de compresión, lo que significa que puede reducir el tamaño de los archivos significativamente sin perder mucha calidad en la compresión.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-3094 de tipo código malicioso integrado (puerta trasera), existe debido a la presencia de una funcionalidad maliciosa integrada en el código de la aplicación (también conocida como puerta trasera) que permite a un atacante remoto obtener acceso no autorizado al sistema.

A. Productos afectados:

- XZ Utils: 5.6.0 - 5.6.1.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados cuando el proveedor lance la última versión para abordar esta vulnerabilidad. Actualmente aún no hay ninguna solución oficial.

Fuente de Información:	• hxxp://access.redhat.com/security/cve/CVE-2024-3094 • hxxp://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094 • hxxp://bugzilla.suse.com/show_bug.cgi?id=1222124

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°076	Fecha: 01-04-2024
		Página: 7 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en IBM Maximo Application Suite		
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 inyección SQL en IBM Maximo Application Suite. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación afectada.

2. DETALLES:

IBM Maximo Application Suite es una plataforma integral de gestión de activos empresariales (EAM) que ofrece una amplia gama de herramientas para la gestión de activos físicos, operaciones, mantenimiento y cumplimiento normativo. La suite está diseñada para ayudar a las organizaciones a optimizar la gestión de sus activos, maximizar la eficiencia operativa y reducir los costos.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-1597 de tipo inyección SQL, existe debido a una limpieza insuficiente de los datos proporcionados por el usuario cuando se utiliza la opción "PreferQueryMode=SIMPLE". Un atacante remoto puede enviar una solicitud especialmente diseñada a la aplicación afectada y ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación.

A. Productos afectados:

- IBM Maximo Application Suite: anterior a la versión 8.8.6.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://www.ibm.com/support/pages/node/7145575

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°076	Fecha: 01-04-2024
		Página: 8 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en Apache Fineract		
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 **MEDIA** de tipo inyección SQL y permisos, privilegios y controles de acceso en Apache Fineract. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación, eludir las restricciones de seguridad y escalar privilegios en una función arbitraria dentro de la aplicación afectada.

2. DETALLES:

Apache Fineract es una plataforma de software de código abierto diseñada para brindar servicios financieros digitales a poblaciones no bancarizadas o sub-bancarizadas en todo el mundo. Desarrollado por la Apache Software Foundation, Fineract ofrece una amplia gama de funciones para la gestión de instituciones financieras, incluyendo la gestión de clientes, cuentas, préstamos, ahorros, y mucho más.

Las vulnerabilidades de severidad **media,** identificadas por MITRE como CVE-2024-23539 y CVE-2024-23538 de tipo, inyección SQL, existe debido a una limpieza insuficiente de los datos proporcionados por los usuarios. Un usuario remoto puede enviar una solicitud especialmente diseñada a la aplicación afectada y ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-23537 de tipo permisos, privilegios y controles de acceso, existe debido a que la aplicación no impone restricciones de seguridad adecuadamente, lo que conduce a eludir las restricciones de seguridad y a una escalada de privilegios a una función arbitraria dentro de la aplicación.

A. Productos afectados:

- Fineract: versión 1.0.0 - 1.8.4.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://cwiki.apache.org/confluence/display/FINERACT/Apache+Fineract+Security+Report • hxxp://lists.apache.org/thread/g8sv1gnjv716lx2h89jbvjdgtrrjmy7h • hxxp://lists.apache.org/thread/by32w2dylzgbqm5940x3wj7519wolqxs • hxxp://lists.apache.org/thread/fq1ns4nprw2vqpkwwj9sw45jkwxmt9f1

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°076**	**Fecha: 01-04-2024**
		Página: 9 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en productos Keyence Corporation		
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 **ALTA** de tipo escritura fuera de límites y lectura fuera de límites en productos Keyence Corporation. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto divulgar información o ejecutar código arbitrario.

2. DETALLES:

Keyence Corporation es una empresa líder en el desarrollo y fabricación de productos de automatización industrial y sistemas de medición de precisión. Keyence se ha destacado por su enfoque en la innovación tecnológica y la calidad de sus productos. frece una amplia gama de productos, que incluyen sensores, sistemas de visión artificial, láseres, microscopios digitales, controladores de movimiento, sistemas de medición de coordenadas y mucho más. Estos productos se utilizan en una variedad de industrias, como la automotriz, la electrónica, la alimentaria, la farmacéutica y la manufacturera en general.

Las vulnerabilidades de severidad **alta,** identificadas por MITRE como CVE-2024-29218 y CVE-2024-29219 de tipo escritura fuera de límites y lectura fuera de límites respectivamente, podrían permitir divulgar información o ejecutar código arbitrario haciendo que un usuario del producto afectado abra un archivo especialmente diseñado.

A. Productos afectados:

- KV Studio, v11.64 y anteriores.
- KV Replay, Viewer v2.64 y anteriores.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://jvn.jp/en/vu/JVNVU95439120/index.html

Índice alfabético