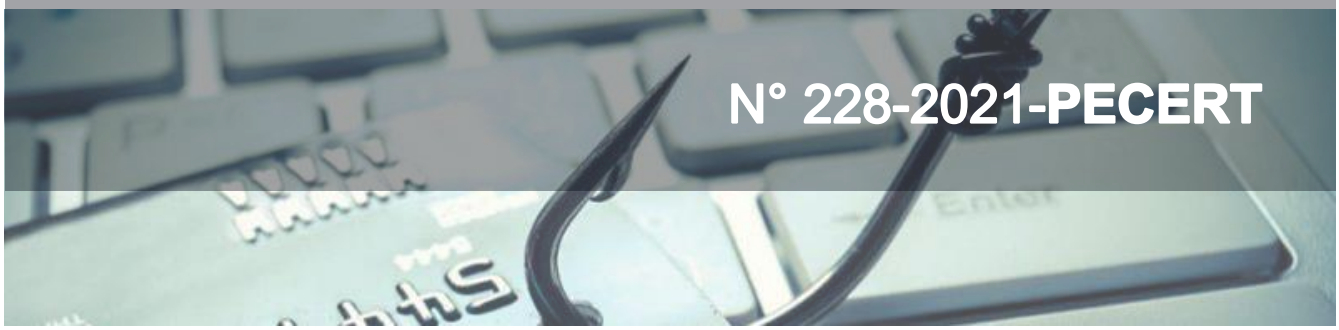
PERÚ | Presidencia del Consejo de Ministros | Secretaria de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Lima, 6 de setiembre de 2021



N° 228-2021-PECERT

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 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 007-2021**.

La presente Alerta Integrada de Seguridad Digital es información especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 228	Fecha: 06-09-2021
		Página: 3 de 11

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS / CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO DEL PERÚ**			
Nombre de la alerta	Atlassian Confluence explotado activamente para instalar criptomineros			
Tipo de ataque	Malware		Abreviatura	Malware
Medios de propagación	USB, disco, red, correo, navegación de internet			
Código de familia	C	Código de subfamilia	C03	
Clasificación temática familia	Código malicioso			

Descripción

1. El 06 de setiembre de 2021, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tomó conocimiento a través de la publicación realizada en la página web "BleepingComputer" los intentos de explotación masiva en curso dirigidos a una vulnerabilidad de seguridad crítica ahora parcheada que afecta las implementaciones de Atlassian Confluence que podrían ser abusadas por atacantes no autenticados para tomar el control de un sistema vulnerable.
2. Confluence es un software de colaboración en equipo. Escrito en Java y utilizado principalmente en entornos corporativos, está desarrollado y comercializado por Atlassian. Confluence se vende tanto como software de uso local como solución de servidor.
3. Los piratas informáticos están explorando activamente y explotando una vulnerabilidad de ejecución remota de código de Atlassian Confluence recientemente revelada para instalar criptomineros después de que se lanzara públicamente un exploit de PoC.

4. Atlassian emitió un aviso de seguridad para una vulnerabilidad de ejecución remota de código (RCE) de Confluence rastreada como CVE-2021-26084 y tiene una calificación de gravedad de 9,8 sobre 10 en el sistema de puntuación CVSS, afecta a todas las versiones anteriores a la 6.13.23, 7.4.11, 7.11.6, 7.12.5 y 7.13.0, lo que permite a un atacante no autenticado ejecutar comandos de forma remota en un servidor vulnerable.
5. Existe una vulnerabilidad de inyección OGNL que permitiría a un usuario autenticado, y en algunos casos a un usuario no autenticado, ejecutar código arbitrario en una instancia de Confluence Server o Data Center, explica el aviso CVE-2021-26084 de Atlassian.
6. Poco después de que se publicaran el artículo y la PoC, las empresas de ciberseguridad comenzaron a informar que los actores de amenazas y los investigadores de seguridad estaban escaneando y explotando activamente los servidores Confluence vulnerables. Sin embargo, la firma de inteligencia de ciberseguridad Bad Packets vió una actividad más nefasta con actores de amenazas de varios países que explotaban servidores para descargar y ejecutar scripts de shell de PowerShell o Linux.
7. A partir de muestras de las vulnerabilidades publicadas por Bad Packets, BleepingComputer confirmó que los actores de amenazas están intentando instalar criptomineros en los servidores Confluence de Windows y Linux.
8. Recomendaciones:
   - Instalar las últimas actualizaciones de su website oficial.
   - Mantener actualizado el antivirus.

Fuentes de información	▪ hxxps://us-cert.cisa.gov/ncas/current-activity/2021/09/03/atlassian-releases-security-updates-confluence-server-and-data ▪ hxxps://www.bleepingcomputer.com/news/security/atlassian-confluence-flaw-actively-exploited-to-install-cryptominers/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 228	Fecha: 06-09-2021
		Página: 4 de 11

Componente que reporta	**GRUPO DE OPERACIONES EN EL CIBERESPACIO DE LA FUERZA AÉREA DEL PERÚ**		
Nombre de la alerta	PrintNightmare: vulnerabilidad en el Administrador de Trabajos de Impresión de Windows		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento e intrusión		

Descripción

1. El 06 de setiembre de 2021, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tomó conocimiento que PrintNightmare continúa siendo explotada por ciberdelincuentes y aprovecha las vulnerabilidades CVE-2021-1675 y CVE-2021-34527.
2. Es preciso indicar, que la actualización de seguridad de Microsoft publicada en junio cerró la CVE-2021-1675, pero no la CVE-2021-34527. A consecuencia de esto, los ciberdelincuentes pueden aprovechar las vulnerabilidades contra ordenadores o servidores con Sistema Operativo Windows que no estén parchados para obtener su control, ya que el Administrador de Trabajo de Impresión se activa en forma predeterminada en dichos sistemas.
3. Las vulnerabilidades antes mencionadas y su explotación se detallan a continuación:
4. CVE-2021-1675 es una vulnerabilidad de elevación de privilegio. Permite que un atacante con privilegios de acceso de bajo nivel cree y utilice un archivo malicioso DLL para ejecutar un exploit y obtener privilegios más elevados. Sin embargo, esto solo es posible si el atacante ya tiene acceso directo al ordenador vulnerable en cuestión. Microsoft considera que esta vulnerabilidad tiene un riesgo relativamente bajo.
5. CVE-2021-34527 es mucho más peligrosa: Si bien es similar, se trata de una vulnerabilidad de ejecución de código remoto (RCE), lo que significa que permite la ejecución remota de archivos DLL. Microsoft ya ha visto exploits de esta vulnerabilidad en entornos no controlados, y Securelist proporciona una descripción técnica más detallada de ambas vulnerabilidades y sus técnicas de explotación.
6. Debido a que los ciberdelincuentes pueden utilizar PrintNightmare para acceder a los datos en la infraestructura corporativa, también pueden utilizar el exploit para ataques de ransomware.
7. Recomendaciones:
   - Actualizar los Sistemas Operativos.
   - Desactivar el administrador de trabajos de impresión de Windows, mismo que viene activado en forma predeterminada.

Fuentes de información	hxxps://bit.ly/3BMIu8J

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 228**	**Fecha: 06-09-2021**
		Página: 5 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en el software SoftController de ABB		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intrusión		

Descripción

1. Resumen:

   El investigador Flavian Dola de AIRBUS, ha reportado una vulnerabilidad de severidad CRÍTICA de tipo falta de control de acceso y de validación de datos de entrada que afecta a SoftController de ABB. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto inyectar y ejecutar código arbitrario en un equipo afectado.

2. Detalles:

   El SoftController es una herramienta de prueba y depuración que se utiliza para las pruebas básicas de programas durante la ingeniería. También se utiliza para 800xA Simulator y APC.

   La vulnerabilidad registrada como CVE-2021-24672 se debe a la falta de un control de acceso y una validación de los datos de entrada en SoftController. La explotación de esta vulnerabilidad podría permitir a un atacante remoto no autenticado, inyectar y ejecutar código arbitrario en un ordenador que ejecuta el software afectado, mediante el envío de un mensaje especialmente diseñado. El código se ejecutará con los privilegios del usuario que inició SoftController.

   Un atacante podría intentar aprovechar la vulnerabilidad creando un mensaje especialmente diseñado y enviándolo a una computadora que ejecute SoftController. Esto requeriría que el atacante tenga acceso a la misma red que la computadora afectada, conectándose a la red ya sea directamente o a través de un firewall configurado o penetrado incorrectamente, o que el atacante instale software malicioso en un nodo de esta red.

   El SoftController normalmente se inicia a petición del usuario que ha iniciado sesión. La vulnerabilidad no está presente cuando SoftController no se está ejecutando. Se recomienda a los clientes que lo inicien solo cuando sea necesario. Además, cuando un proyecto se ha descargado en SoftController, no aceptará un mensaje genérico que pueda aprovechar la vulnerabilidad. Un atacante necesitaría crear mensajes de ataque específicos.

3. Productos afectados):

   ABB Base Software para SoftControl, todas las versiones hasta la 6.1.

4. Solución:

   ABB recomienda actualizar el software afectado a la versión System 800xA 6.1.1, cuando esté disponible. Además, exhorta a aplicar las siguientes medidas:

   - Ejecutar el software solo cuando sea necesario, en el momento justo antes de descargar un proyecto o en un entorno controlado con conexiones limitadas;
   - Habilitar la función InhibitDownload para evitar descargas al software;
   - Coloque los sistemas de control en una red de control dedicada que contenga únicamente sistemas de control;
   - Ubique redes y sistemas de control detrás de firewalls y sepárelos de cualquier otra red, como las redes comerciales e Internet;
   - Bloquear cualquier tráfico entrante de Internet destinado a las redes / sistemas de control;
   - Limite el tráfico de Internet saliente que se origina en los sistemas / redes de control tanto como sea posible;

- Limitar la exposición de las redes / sistemas de control a los sistemas internos. Adapte las reglas del cortafuego que permitan el tráfico desde sistemas internos para controlar redes / sistemas para permitir solo IP de origen, IP de destino y puertos de servicio / destino que definitivamente son necesarios para la operación de control normal;
- Cree reglas estrictas de firewall para filtrar las vulnerabilidades del sistema de control de objetivos de tráfico de red malicioso ("explotar el tráfico");
- Cerrar el puerto TCP 102 en Windows firewall o en su defecto, proteger la red contra accesos no autorizados.

Fuentes de información	▪ hxxps://www.incibe-cert.es/alerta-temprana/avisos-sci/ejecucion-remota-codigo-base-software-softcontrol-abb ▪ hxxps://search.abb.com/library/Download.aspx?DocumentID=2PAA122974&LanguageCode=en&DocumentPartId=&Action=Launch

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 228**	**Fecha: 06-09-2021**
		Página: 7 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**			
Nombre de la alerta	Múltiples vulnerabilidades críticas “BrakTooth” afectan a dispositivos Bluetooth Link Manager			
Tipo de ataque	Explotación de vulnerabilidades conocidas		Abreviatura	EVC
Medios de propagación	Red, internet			
Código de familia	H	Código de subfamilia	H01	
Clasificación temática familia	Intrusión			

Descripción

1. Resumen:

   Investigadores de la Universidad de Tecnología y Diseño de Singapur (SUTD) han descubierto una nueva familia de vulnerabilidades de severidad crítica en Bluetooth Link Manager denominada “BrakTooth” que van desde la denegación de servicio (DoS) a través de las fallas (crashes) de firmware y puntos muertos (deadlocks) en el hardware de los productos básicos a la ejecución de código arbitrario (ACE) en ciertos dispositivos de Internet de las cosas (IoT). La explotación exitosa de estas vulnerabilidades podría permitir que un atacante en el rango de radio active interbloqueos, bloqueos o ataques de ACE. La vulnerabilidad BrakTooth crea una amplia superficie de ataque a miles de millones de dispositivos en todo el mundo que incorporan chips de proveedores como Intel, Infineon (Cypress), Silicon Labs, Qualcomm, entre otros.

2. Detalles:

   La nueva familia de vulnerabilidades BrakTooth afecta a los dispositivos habilitados para Bluetooth al bloquearlos o bloquearlos continuamente, mientras que algunas tienen consecuencias más graves, como la ejecución de código arbitrario.

   Según los investigadores, el impacto de las vulnerabilidades descubiertas se clasifica en bloqueos e interbloqueos. Los bloqueos generalmente desencadenan una afirmación fatal, fallas de segmentación debido a un desbordamiento de búfer o del montón dentro del firmware del SoC. Los interbloqueos, por el contrario, llevan al dispositivo de destino a una condición en la que no es posible ninguna otra comunicación BT. Esto puede suceder debido a que el escaneo de paginación se deshabilita a la fuerza (Interbloqueo de escaneo de paginación), la corrupción de la máquina de estado en desbordamiento o la deshabilitación total de la funcionalidad BT a través de la ACE en la ejecución de páginas de funciones.

   Por otro lado, los investigadores señalaron que la explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar funciones arbitrarias o incluso causar un punto muerto en el que se requeriría un reinicio manual, interrumpir la conexión Bluetooth y evitar que los dispositivos externos se conecten al dispositivo, podría bloquear el dispositivo y provocar la DoS, interrumpir la conexión Bluetooth o incluso causar un interbloqueo en el que se requeriría un reinicio manual, interrumpir la conexión Bluetooth y evitar que los dispositivos externos se conecten al dispositivo.

   CVE-2021-28139, CVE-2021-34144, CVE-2021-28136, CVE-2021-28135, CVE-2021-28155, CVE-2021-31717, CVE-2021-31609, CVE-2021-31612, CVE-2021-34150, CVE-2021-31613, CVE-2021-31611, CVE-2021-31785, CVE-2021-31786, CVE-2021-31610, CVE-2021-34149, CVE-2021-34146, CVE-2021-34143, CVE-2021-34145, CVE-2021-34148, CVE-2021-34147.

3. Productos afectados:

   Los dispositivos afectados incluyen dispositivos IoT, como concentradores domésticos inteligentes, módulos, teléfonos inteligentes, computadoras portátiles y dispositivos de audio que utilizan implementaciones clásicas de Bluetooth vulnerables.

Los fabricantes afectados son: Espressif Systems, Harman International, Infineon, Silabs, Bluetrum, Zhuhai Jieli Technology, Actions Technology, Qualcomm, Texas Instruments e Intel.

4. Solución:

Se recomienda a los usuarios y administradores de los productos afectados que instalen inmediatamente las últimas actualizaciones de seguridad de los respectivos fabricantes. Si las actualizaciones no están disponibles, se recomienda a los usuarios y administradores que consulten el sitio web de los respectivos fabricantes con regularidad para obtener actualizaciones y acciones recomendadas. Según el caso, se podría considerar apagar el protocolo de comunicaciones Bluetooth del dispositivo cuando no esté en uso como una medida de mitigación temporal.

Fuentes de información	

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 228	Fecha: 06-09-2021
		Página: 9 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Detección de Malware en el aplicativo ImageEditor			
Tipo de ataque	Malware		Abreviatura	Malware
Medios de propagación	USB, disco, red, correo, navegación de internet.			
Código de familia	C	Código de subfamilia	C03	
Clasificación temática familia	Código malicioso			

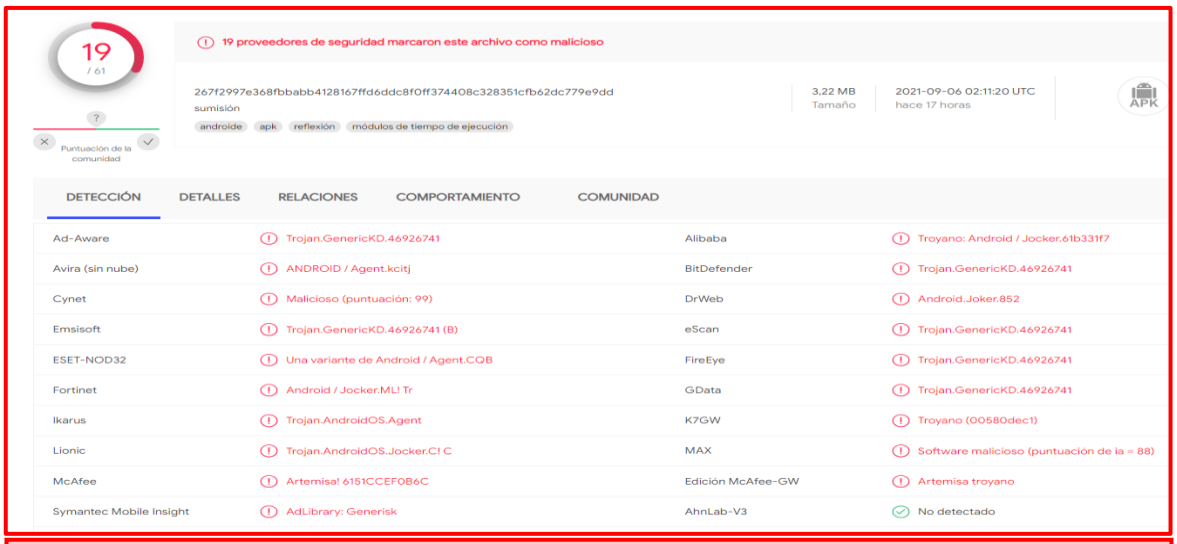
Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento que actores de amenazas vienen distribuyendo e infectando dispositivos móviles con el malware Joker mediante el aplicativo “ImageEditor” que se encuentra disponible en la plataforma de distribución digital de aplicaciones móviles para los dispositivos con sistema operativo Android “Google Play Store”.
2. La aplicación “ImageEditor” permite realizar mejoras a los archivos de imágenes, tales como fotografías, dibujos, gráficos o colocar textos en las imágenes editadas; sin embargo, la víctima al descargar el aplicativo concede permisos especiales en el menú de accesibilidad de Android, de tal manera el malware conocido como “Joker” se puede ejecutar de varias formas como realizar suscripciones premium de cualquier servicio, así como instalar software espía en el terminal de los dispositivos móviles, afectando los datos sensibles de las víctimas.
3. Detalles del Aplicativo móvil “ImageEditor”
   - Versión : 1.0.831
   - Tamaño de archivo : 4,1 MB
   - Nombre del paquete : com.configuration.imageeditor
   - Actualizado : 31AGO21
   - Requiere de Android : 6,0 +
   - Precio : Gratis

4. Permisos solicitados:
   - Calendario
     - Leer los eventos del calendario y la información confidencial
   - Contactos
     - Encontrar cuentas en el dispositivo
     - Leer tus contactos
   - Teléfono
     - Leer el estado del teléfono y la identidad
   - Fotos/multimedia/archivos
     - Acceder al sistema de archivos del almacenamiento USB
     - Leer el contenido de su memoria USB
     - Modificar o eliminar el contenido de su almacenamiento USB
   - Almacenamiento
     - Leer el contenido de su memoria USB
     - Modificar o borrar el contenido de su memoria USB
   - Cámara
     - Hacer fotos y vídeos
   - Información sobre la conexión
     - Wi-Fiver las conexiones Wi-Fi
   - Otros
     - Ver las conexiones de red
     - Cambiar la conectividad de la red

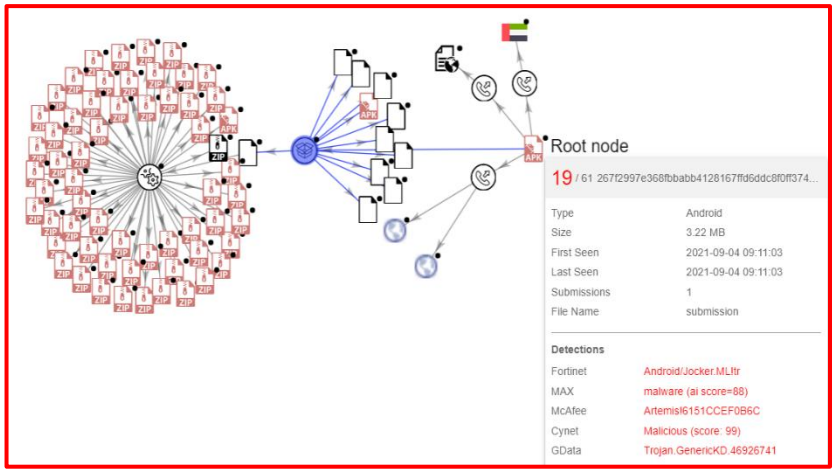
- Acceso total a la red
- Ejecutar al inicio

5. Análisis del paquete **com.configuration.imageeditor** del aplicativo "ImageEditor", en las diferentes plataformas virtuales de seguridad digital a fin de determinar el grado de confianza y la detección de algún malware que pudiera poner en riesgo a los dispositivos Android, obteniendo como resultado:



Observación: Se detecta que el archivo APK contiene Malware uno de ellos conocido como "Joker" que está diseñado para robar mensajes SMS, lista de contactos e información del dispositivo, además de suscribir de manera oculta a usuarios en servicios de pago.

- MD5 : 6151ccef0b6c839616c2e54099f607eb
- SHA-1 : f623cdc6d4d04968e630001eb76922cb3e7472f7
- SHA-256 : 267f2997e368fbbabb4128167ffd6ddc8f0ff374408c328351cfb62dc779e9dd
- Topología



6. Recomendaciones:
   - Desinstalar la aplicación del dispositivo móvil si lo tiene instalado.
   - Verifica la información de los aplicativos móviles visitando el sitio web de los desarrolladores.
   - Analizar los permisos otorgados a las aplicaciones móviles.
   - No abrir o descargar archivos sospechosos.
   - Mantenga su antivirus actualizado.
   - Realizar las actualizaciones correspondientes desde fuentes originales.

Fuentes de información	Análisis propio de redes sociales y fuente abierta

Índice alfabético