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, 10 de noviembre de 2023

269-2023-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°269	Fecha: 10-11-2023
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Comunicado de Seguridad de la Información - Recuperación de cuentas de WhatsApp		
Tipo de Ataque	Robo de información	Abreviatura	RobInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K01
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

El robo de cuentas de WhatsApp es un fraude que se ha vuelto mucho más recurrente en todo el mundo. Los cibercriminales han estado utilizando todo tipo de excusas para robar el código de verificación de seis dígitos que WhatsApp envía vía SMS -y también mediante llamada- cada vez que abrimos WhatsApp en un nuevo teléfono.

Una vez que obtienen el código, acceden a las cuentas y se comunican con los contactos de las víctimas haciéndose pasar por el titular para solicitar dinero ante una supuesta emergencia. Lamentablemente, muchas personas han caído en la trampa. Convencidas de que están hablando con un familiar, amigo o conocido, hacen transferencias de dinero con la intención de ayudar a estas personas, pero nunca se imaginan que del otro lado hay un criminal que tomó el control de la cuenta.

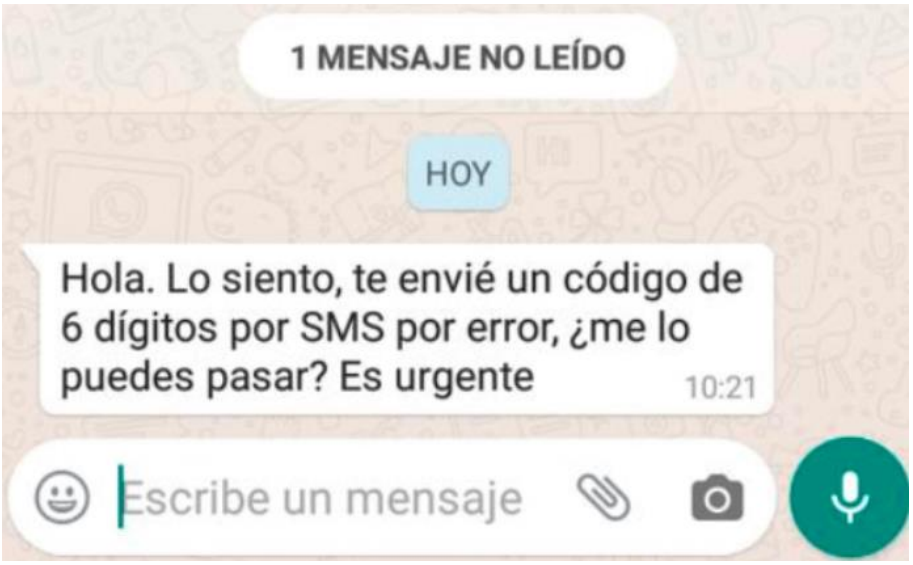
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) del Ministerio del Interior y Seguridad Pública de Chile comparte algunas recomendaciones en caso de que alguien tome control de tu cuenta de WhatsApp.

2. DETALLES:

La solicitud del código de verificación que envían los cibercriminales puede llegar por diferentes caminos. Puede ser un mensaje que llega de un contacto desconocido que, utilizando alguna excusa, solicita que reenvíen un código que por error llegó a su número, o incluso puede ser un contacto conocido quien solicita el código. En este caso se trata de una persona que fue víctima del robo de la cuenta y solicita el código simulando ser el titular de la cuenta.

Recuerda que tu código de verificación de WhatsApp es personal y no debe ser compartido con nadie. Si por algún motivo te engañaron y compartiste tu código de verificación, perderás el acceso a tu cuenta de WhatsApp.

Con el tiempo hemos visto que los cibercriminales han explorado otras formas de ingeniería social para que las excusas suenen más creíbles. Por ejemplo, se hacen pasar por soporte técnico de WhatsApp para informar que es necesario verificar su cuenta debido a una actividad sospechosa en su cuenta.



Si bien lo más común es que los ciberdelincuentes busquen convencer a la persona mediante un mensaje o llamada para que compartan el código que llega vía SMS, como mencionamos antes, WhatsApp también ofrece la opción de enviar el código de verificación de seis dígitos a través de una llamada. Los cibercriminales saben esto y también lo aprovechan para obtener el código. ¿Cómo? Lo que hacen los delincuentes al intentar registrar tu cuenta de WhatsApp desde otro dispositivo es solicitar que el envío del código sea a través de una llamada. Si la víctima no contesta la llamada WhatsApp o la línea está ocupada, WhatsApp deja el código como mensaje de voz en el buzón de voz. Y lo que muchas personas no saben es que con algunos operadores de telefonía puede resultar sencillo para un delincuente acceder al buzón de voz de un número, sobre todo porque muchas personas no tienen configurado el acceso al buzón de voz con una clave PIN o no cambiaron la que viene por defecto.

En algunos casos hemos visto que los estafadores suelen recurrir al método de la llamada en horas de la madrugada aprovechando que la mayoría de las personas duermen y probablemente no atiendan el teléfono.

3. RECOMENDACIONES:

- Activar la autenticación en dos pasos en la app.
- Notificar a los familiares y amigos por teléfono, ya sea en persona o por otro medio, en el caso que hayas compartido tu código de verificación. ya que la cuenta podría ser utilizada para fraudes, estafas o suplantaciones de identidad.
- Para recuperar la cuenta de WhatsApp:
  - Registrarse nuevamente con tu número de teléfono e ingresa el código de 6 dígitos que recibirás por SMS o llamada telefónica. Este código es la única forma de confirmar que eres el dueño del número y debes poder recibirlo en tu teléfono.
  - Una vez ingresado el código de 6 dígitos, la sesión de la persona con acceso a tu cuenta se cerrará automáticamente.
  - En caso de que no recibas el código, te sugerimos bloquear temporalmente tu línea telefónica con tu compañía de teléfonos.
  - Es posible que te pida ingresar un código de verificación en dos pasos. Si no sabes ese código, es posible que la persona con acceso a tu cuenta haya activado este mecanismo. En ese caso, debes esperar siete días para poder acceder sin el código de verificación en dos pasos. Independientemente de si sabes el código de verificación en dos pasos o no, la sesión de la persona con acceso a tu cuenta se cerrará en cuanto ingreses el código de 6 dígitos enviado.

Fuente de Información:	• hxxps://csirt.gob.cl/noticias/10cnd23-00120-01/ • hxxps://www.welivesecurity.com/la-es/2023/01/30/robo-cuentas-whatsapp-tendencia-crece-podcast/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°269	Fecha: 10-11-2023
		Página: 6 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de corrupción de memoria en el análisis del encabezado del host del servidor HTTP uC-HTTP integrado de Weston		
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 restricción inadecuada de operaciones dentro de los límites de un búfer de memoria en el análisis del encabezado del host del servidor HTTP uC-HTTP integrado de Weston. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución de código arbitrario.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2023-31247 de tipo restricción inadecuada de operaciones dentro de los límites de un búfer de memoria en la funcionalidad de análisis de encabezados del host del servidor HTTP de Weston Embedded uC-HTTP v3.01.01. Un paquete de red especialmente diseñado puede provocar la ejecución de código. Un atacante puede enviar un paquete malicioso para desencadenar esta vulnerabilidad.

La implementación del servidor uC-HTTP está diseñada para usarse en sistemas integrados que ejecutan los núcleos RTOS µC/OS II o µC/OS III. Este servidor HTTP admite muchas funciones que incluyen conexiones persistentes, procesamiento de formularios, codificación de transferencia fragmentada, procesamiento de campos de encabezado HTTP, procesamiento de cadenas de consulta HTTP y contenido dinámico.

A. Productos afectados:

- Weston Embedded uC-HTTP v3.01.01.
- Weston Embedded Cesium NET 3.07.01.
- Silicon Labs Gecko Platform 4.3.1.0.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://www.talosintelligence.com/vulnerability_reports/TALOS-2023-1746 • hxxps://weston-embedded.com/micrium/overview • hxxps://www.silabs.com/developers/gecko-software-development-kit

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°269**	**Fecha: 10-11-2023**
		Página: 7 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad alta en el software FreeBSD libc		
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 montón en el software FreeBSD libc. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-5941 de tipo desbordamiento de búfer basado en montón, existe debido a un error de límite dentro de la función __sflush() en libc. Un atacante remoto puede pasar datos especialmente diseñados a la aplicación que utiliza la biblioteca afectada, desencadenar un desbordamiento de búfer basado en el montón y ejecutar código arbitrario en el sistema de destino. La vulnerabilidad se puede utilizar para escalar privilegios o ejecutar código arbitrario de forma remota. El vector de ataque depende de la aplicación o demonio que utiliza la versión vulnerable de libc.

A. Productos afectados:

- FreeBSD: versión 12.4 - 14.0.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://security.freebsd.org/advisories/FreeBSD-SA-23:15.stdio.asc

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°269**	**Fecha: 10-11-2023**
		Página: 8 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en Apache Traffic Server		
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 error de validación de entrada y divulgación de información en Apache Traffic Server. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto realizar un ataque de denegación de servicio (DoS) y obtener acceso a información potencialmente confidencial.

2. DETALLES:

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-39456 de tipo error de validación de entrada, existe debido a una validación insuficiente de la entrada proporcionada por el usuario al manejar tramas HTTP/2. Un atacante remoto puede enviar solicitudes HTTP especialmente diseñadas a la aplicación y realizar un ataque de DoS.

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-41752 de tipo divulgación de información, existe debido a la salida excesiva de datos por parte de la aplicación. Un atacante remoto puede obtener acceso no autorizado a información confidencial del sistema.

A. Productos afectados:

- Apache Traffic Server: 9.0.0 - 9.2.2.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://lists.apache.org/thread/5py8h42mxfsn8l1wy6o41xwhsjlsd87q • hxxp://www.debian.org/security/2023/dsa-5549

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°269**	**Fecha: 10-11-2023**
		Página: 9 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en productos Weidmueller		
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 búfer en productos Weidmueller. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante obtener acceso completo al servidor afectado o escalar privilegios.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2023-3935 de tipo desbordamiento de búfer en el servicio de red Wibu CodeMeter Runtime podría permitir a un atacante, no autenticado, realizar una ejecución remota de código y obtener acceso completo al sistema *host* y escalar privilegios en el servicio de red Wibu CodeMeter Runtime podría permitir a un atacante, no autenticado, realizar una ejecución remota de código y obtener acceso completo al sistema *host* y escalar privilegios.

A. Productos afectados:

- Versiones 2.0.0 y 2.0.1 de los productos:
  - IOT-GW30-4G-EU (con u-OS).
  - IOT-GW30 (con u-OS).
  - UC20-WL2000-AC (con u-OS).
  - UC20-WL2000-IOT (con u-OS).
- U-create studio, versiones 4.2.4 y anteriores.

3. RECOMENDACIÓN:

- Actualizar los productos afectados con las últimas versiones de software disponibles que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://cert.vde.com/de/advisories/VDE-2023-032/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°269	Fecha: 10-11-2023
		Página: 10 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de sitio web fraudulento del Banco Crédito del Perú		
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		

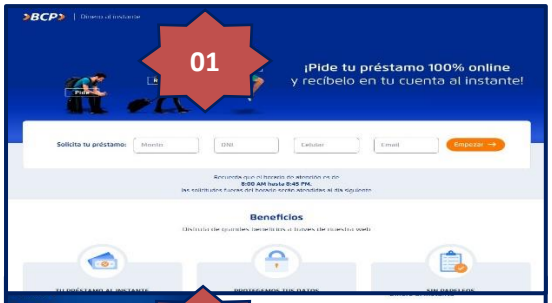
Descripción

1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen realizando una campaña de Phishing, suplantando el sitio web del Banco de Crédito del Perú (servicio online de préstamo personal), con la finalidad de robar información bancaria de los usuarios de la entidad financiera como números de tarjetas bancarias, clave intranet de seis dígitos, documento de identidad, correo electrónico, etc.

2. DETALLES:

El proceso del Phishing es el siguiente:



Paso N.º 01

Solicitan a la víctima registrar lo siguiente:

- El monto solicitado del préstamo.
- Documento Nacional de identidad (DNI).
- Número de Celular.
- Correo electrónico.

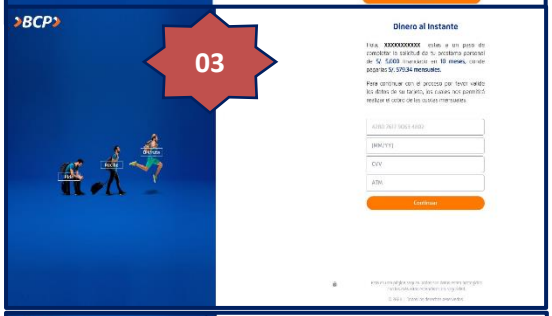
Para luego dar clic en <**Empezar**>

Paso N.º 02

Instan a la víctima que registre datos como:

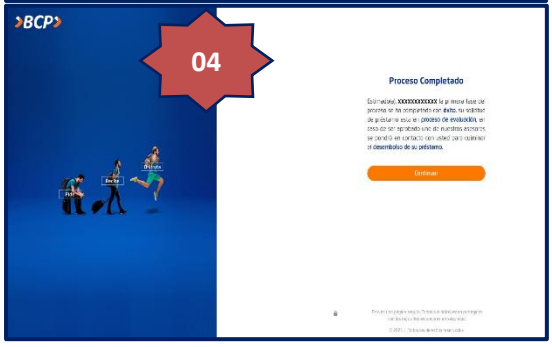
- El número de la tarjeta bancaria.
- Clave de seis dígitos del intranet.
- Código captcha.

Para luego dar clic en <**Continuar**>.



Paso N.º 03

Una vez brindado los datos solicitados en el paso N.º 02, aparece una pantalla requiriendo información de la tarjeta bancaria como la fecha de expedición, el código de seguridad (CVV) y la clave de cuatro dígitos utilizado en el cajero automático, para luego dar clic en <**Continuar**>.



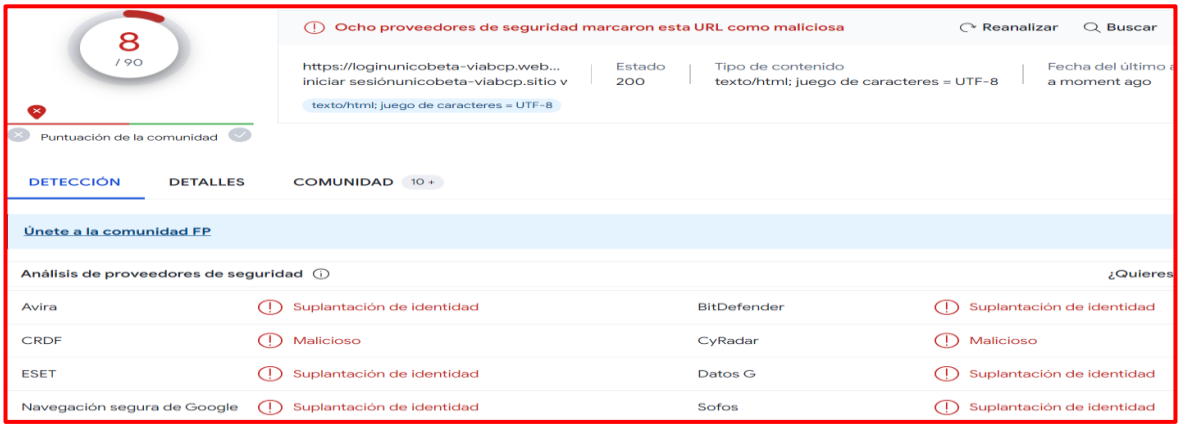
Paso N.º 04

Luego, aparece una pantalla indicando que se ha completado con éxito el registro de datos y en el transcurso del día asesores de la entidad bancaria se pondrán en contacto con la víctima, para luego dar clic en <**Continuar**>. Redirigiendo al sitio web oficial de la entidad bancaria; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

A. Comparación del sitio web oficial y fraudulento.

- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

B. Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.



C. Indicadores de compromiso (IoC)

- Dominio : unicobeta-viabcp.website
- Servidor : LiteSpeed
- SHA-256 : 3d5279e58f9b26d53d4fd5cab08fa6d157ec15c5e6cd60b7809bad4c2acbf534
- IP : 195[.]179[.]237[.]114
- Tipo de tex. : Text/Html

3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- No aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.

Índice alfabético