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

247-2024-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°247	Fecha: 25-10-2024
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Ofertas de empleo falsas circulan por WhatsApp		
Tipo de Ataque	Phishing		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 altos índices de desempleo hacen que muchas personas estén desesperadas por conseguir trabajo. Muchos son tentados a aceptar propuestas que les llegan por Whatsapp, de trabajos que prometen ser sencillos, con requisitos fáciles para aplicar y con la posibilidad de laborar desde casa.

2. DETALLES:

Las falsas ofertas de empleo por WhatsApp se han convertido en una constante: los cibercriminales se valen del renombre de ciertas marcas o empresas para hacer ofrecimientos de puestos laborales inexistentes, con el único objetivo de obtener los datos personales de sus víctimas o algún rédito económico.

Ofrecen un empleo atractivo de medio tiempo realizando tareas con el teléfono a cambio de comisiones.

Camilo Gutiérrez Amaya, jefe del Laboratorio de Investigación de ESET Latinoamérica, destaca que estos mensajes suelen incluir características sospechosas y agrega que grandes empresas rara vez contactan a posibles empleados a través de WhatsApp.

Algunos estafadores piden dinero inicial, mientras que otros envían enlaces a supuestas plataformas de trabajo, generando una fachada de seriedad que muchas veces confunde a quienes desconocen los indicios comunes de estos fraudes.

Además del fraude, estas prácticas se vinculan con redes de trata de personas que buscan enganchar a mujeres y migrantes. Estas plataformas digitales sirven de herramientas frecuentes a los tratantes debido al anonimato que ofrecen y que les permite iniciar contacto con potenciales víctimas mediante supuestas entrevistas de trabajo.

Según la Organización Internacional para las Migraciones (OIM), solo 60% de la actividad en Internet proviene de personas, mientras que el 40% restante lo generan bots que redirigen el tráfico a sitios engañosos para robar datos bancarios o realizar otras estafas.

Los delincuentes que solicitan pagos por adelantado logran convencer a sus víctimas por el servicio de iniciar procesos de colocación, agendar entrevistas o asegurar contrataciones. Exigen depósitos bancarios para emitir contratos, proporcionar credenciales de empleado o finalizar la contratación. Además, buscan recolectar información personal y sensible de las víctimas.

Las estafas más comunes a través de WhatsApp:

Amazon.- La compañía identificó un ejemplo en el que una supuesta recepcionista de la mundialmente conocida empresa Amazon contacta a una persona, sin saber siquiera su nombre, para que comience a trabajar mediante un formato de comisiones.

Mercado Libre.- El nombre de Mercado libre también es utilizado por los ciberatacantes para generar interés en sus posibles víctimas, con salarios altos y mínimos esfuerzos.

En estos casos, la supuesta reclutadora busca generar confianza acreditando su vínculo con Mercado Libre mediante un supuesto código de empleada y una foto de la credencial.

Otro ejemplo que también se vale de Mercado Libre para generar interés, es el supuesto “Gerente de Atención al Cliente” que detalla las tareas que la víctima debería desempeñar.

Temu.- Otra característica que suelen tener las falsas ofertas de empleo es cuando el supuesto reclutador pide un ingreso inicial de un dinero por parte de la víctima; por otro lado, el mensaje recibido, supuestamente de un "reclutador" contiene un enlace a una plataforma para comenzar a trabajar.

Shein.- La plataforma de ventas por internet presente en 150 países del mundo también es utilizada para realizar engaños. Y con fórmula conocida: trabajo de medio tiempo y altos ingresos.

Como es habitual en estos engaños, el sistema de supuestas recompensas por comisiones vuelve a hacerse presente. Esta vez, bajo la promesa de trabajar para Shein.

Berksha.- Esta cadena de indumentaria, cuyas oficinas centrales se encuentra en España, también es utilizada como señuelo. En este caso, llama la atención, por ejemplo, que los mensajes figuren como Reenviado.

Facebook.- En este caso la red social creada por Mark Zuckerberg es utilizada para llamar la atención de posibles víctimas. La recompensa salarial es muy sustanciosa, mientras que los requisitos para desempeñar la tarea son nulos.

Tik Tok.- Los estafadores se valen de la reconocida red social y ofertas de ganancias importantes, para llamar la atención de sus víctimas. El supuesto trabajo consiste en seguir a algunas marcas en específico.

YouTube.- También sirve como señuelo para ofrecer supuestas ofertas de trabajo tentadores, con buena paga y que en teoría solo requieren de un clic.

Google Maps.- Como es habitual en este tipo de engaños, los estafadores buscan generar interés con un supuesto trabajo de medio tiempo en Google Maps, con la promesa de ganar dinero fácil desde un dispositivo móvil, dedicando pocos minutos al día.

SnagaJob.- El estafador se hace pasar por la reconocida reclutadora de empleo, con la promesa en que un trabajo simple representará ganancias sustanciales. También utilizan SnagaJob como señuelo para difundir una propuesta de supuestamente trabajar para aumentar las visualizaciones de perfiles en redes sociales de "celebridades".

ZipRecruiter.- La empresa de empleo en línea también es utilizada para una estafa, la cual promete un empleo de medio tiempo y ganancias por demás tentadoras.

3. RECOMENDACIONES:

- Verificar la autenticidad del sitio web revisando que tenga una dirección URL segura (https://) y revisando la legitimidad del dominio. Evitar sitios con nombres extraños o mal escritos, ya que podrían ser indicativos de estafas.
- Desconfiar de las ofertas demasiado buenas para ser verdad. Las estafas suelen ofrecer productos a precios muy bajos o promesas de ganar mucho dinero fácil.
- Comprobar la autenticidad de las redes sociales, buscando señales de actividad genuina, como interacciones con usuarios y publicaciones regulares.
- Utilizar soluciones antiphishing, antimalware en tus dispositivos para aprevenir riesgos de este tipo.
- Capacitar a su equipo en las mejores prácticas de ciberseguridad y mantenerlos informados sobre las tácticas de ingeniería social, esquemas de phishing y últimas amenazas.

Fuente de Información:	• hxxps://www.welivesecurity.com/es/estafas-enganos/ofertas-empleo-falsas-circulan-whatsapp/ • hxxps://www.vanguardia.com/entretenimiento/tendencias/2024/10/27/11-ofertas-de-empleo-falsas-que-circulan-por-whatsapp/ • hxxps://www.elespectador.com/economia/cuidado-con-estas-falsas-ofertas-de-empleo-que-circulan-por-whatsapp/ • hxxps://amexi.com.mx/nacional/falsas-ofertas-empleo-whatsapp/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°247	Fecha: 25-10-2024 Página: 6 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en enrutadores Buffalo WSR-2533DHPL2 y WSR-2533DHP3		
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:

Buffalo Technologies Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo recorrido de ruta en los enrutadores WSR-2533DHPL2 y WSR-2533DHP3. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado realizar ataques de recorrido de directorio omitir la autenticación.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2021-20090 de tipo recorrido de ruta en las interfaces web de los dispositivos de red fabricados por Arcadyan, incluidos los firmwares Buffalo WSR-2533DHPL2 y WSR-2533DHP3, podría permitir a un atacante remoto no autenticados realizar ataques de recorrido de directorio y eludir los mecanismos de autenticación. La vulnerabilidad existe debido a un error de validación de entrada al procesar secuencias de recorrido de directorios en las interfaces web. Un atacante remoto puede enviar una solicitud HTTP especialmente diseñada y eludir los mecanismos de autenticación, lo que podría llevar al control no autorizado de los dispositivos afectados.

Los atacantes pueden aprovechar esta vulnerabilidad para modificar las configuraciones de los dispositivos, como habilitar el acceso a Telnet, lo que facilita la ejecución remota de comandos. Se ha observado que los atacantes utilizan scripts para descargar y ejecutar cargas útiles maliciosas, incluidas variantes de la botnet Mirai.

Se debe de tener en cuenta que esta vulnerabilidad está siendo explotada por la botnet Mirai en agosto de 2021.

A. Productos afectados:

- Buffalo WSR-2533DHPL2: versión de firmware <= 1.02.
- Buffalo WSR-2533DHP3: versión de firmware <= 1.24.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de firmware disponibles que abordan esta vulnerabilidad.
- Implementar soluciones de monitoreo para detectar actividades inusuales que puedan indicar intentos de explotación.
- Aumentar la conciencia entre los usuarios sobre la importancia de las actualizaciones periódicas y las prácticas de seguridad para los dispositivos IoT.

Fuente de Información:	• hxxps://www.tenable.com/security/research/tra-2021-13 • hxxps://www.secpod.com/blog/arcadyan-based-routers-and-modems-under-active-exploitation/ • hxxps://www.kb.cert.org/vuls/id/914124 • hxxps://medium.com/tenable-techblog/bypassing-authentication-on-arcadyan-routers-with-cve-2021-20090-and -enraizando-algunos-búfalos-ea1dd30980c2 • hxxps://www.cybersecurity-help.cz/dashboard/vulnerabilities/exploits/52635/#10754

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°247	Fecha: 25-10-2024 Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Apache Log4j		
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:

Apache Software Foundation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo inyección de código en Apache Log4j, comúnmente conocida como "**Log4Shell"**. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2021-44228 de tipo inyección de código en la biblioteca **Apache Log4j**, que se usa ampliamente para el registro en aplicaciones Java, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada incorrecta al procesar solicitudes LDAP. Un atacante remoto puede enviar una solicitud especialmente diseñada a la aplicación y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

El uso generalizado de Log4j en numerosas aplicaciones y servicios significa que potencialmente cientos de millones de dispositivos podrían verse afectados. Las aplicaciones que dependen de Log4j incluyen marcos populares como Apache Struts, Apache Solr y Elasticsearch.

A. Productos afectados:

- Apache Log4j: 2.0 - 2.14.1.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión 2.16.0 o posterior que aborda esta vulnerabilidad.
- Limitar el acceso saliente a la red desde máquinas potencialmente vulnerables, en el caso que no sea posible realizar una actualización inmediata, e implementar un firewall de aplicaciones web (WAF) y sistemas de detección/prevención de intrusiones (IDS/IPS).

Fuente de Información:	• hxxps://www.lunasec.io/docs/blog/log4j-zero-day/ • hxxps://github.com/apache/logging-log4j2/pull/608 • hxxps://github.com/advisories/GHSA-jfh8 -c2jp-5v3q • hxxps://www.ibm.com/es-es/topics/log4shell • hxxps://cve.org/CVERecord?id=CVE-2021-44228

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°247	Fecha: 25-10-2024 Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Palo Alto PAN-OS		
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:

Palo Alto Networks, Inc. ha publicado una vulnerabilidad de severidad **crítica** de tipo inyección de comandos que afecta a varias versiones del software PAN-OS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar comandos arbitrarios con privilegios de root y comprometer el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-3400 de tipo inyección de comandos en Palo Alto PAN-OS, podría permitir a un atacante remoto ejecutar comandos arbitrarios en el sistema objetivo. La vulnerabilidad existe debido a una validación de entrada incorrecta en la función GlobalProtect. Un atacante remoto no autenticado puede pasar datos especialmente diseñados a la aplicación y ejecutar comandos arbitrarios en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

Palo Alto Networks indico, que hay explotación activa de esta vulnerabilidad, con la instalación de un backdoor conocido como UPSTYLE, que incluye un script malicioso llamadoupdate.py.

A. Productos afectados:

- Palo Alto PAN-OS: 11.1 - 11.1.2-h2, 11.0 - 11.0.4, 10.2 - 10.2.9.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Desactivar las configuraciones de GlobalProtect y la telemetría si no son necesarias.
- Realizar auditorías regulares de seguridad para detectar vulnerabilidades.

Fuente de Información:	• hxxps://security.paloaltonetworks.com/CVE-2024-3400 • hxxps://cve.org/CVERecord?id=CVE-2024-3400

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°247	Fecha: 25-10-2024 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en productos 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:

Microsoft ha actualizado una publicación de una vulnerabilidad de severidad **CRÍTICA** de tipo restricción inadecuada de operaciones dentro de los límites de un búfer de memoria que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2022-21907 de tipo restricción inadecuada de operaciones dentro de los límites de un búfer de memoria que afecta a productos de Microsoft, podría permitir a un atacante remoto la ejecución remota de código (RCE) que afecta a la pila de protocolo HTTP de Microsoft. La vulnerabilidad existe debido a un error de límite en la función HTTP Trailer Support en HTTP Protocol Stack (http.sys). Un atacante remoto puede enviar una solicitud HTTP especialmente diseñada al servidor web, provocar un desbordamiento de búfer y ejecutar código arbitrario en el sistema.

A. Productos afectados:

- Windows: 10 1809 10.0.17763.1, 10 20H2 10.0.19042.572, 10 21H1 10.0.19043.985, 11 21H2 10.0.22000.194.
- Servidores Windows: 2019 10.0.17763.1 - 2022 10.0.20348.202.
- Microsoft IIS: 10.0.

Windows Server 2019 y Windows 10 versión 1809 no son vulnerables de forma predeterminada. A menos que haya habilitado la compatibilidad con HTTP Trailer a través del valor de registro “EnableTrailerSupport”, los sistemas no son vulnerables.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Monitorear patrones de tráfico de red inusuales que puedan indicar intentos de explotar esta vulnerabilidad.

Fuente de Información:	• hxxps://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21907

Índice alfabético