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

202-2024-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°202	Fecha: 02-09-2024
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Fraude a través de plataformas que ofrecen supuestas oportunidades laborales		
Tipo de Ataque	Portal fraudulento	Abreviatura	PortalFrau
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G02
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Las víctimas son engañadas para hacer tareas por Internet e invertir en una plataforma virtual que está controlada por los estafadores. Cuando quieren cobrar el dinero de sus labores, no les permiten retirar sus ganancias.

2. DETALLES:

Esta modalidad de fraude consiste en anuncios que captan personas para realizar trabajos remotos en distintas plataformas de ventas, que luego de aceptar la propuesta son engañadas para invertir en las plataformas en base a un esquema Ponzi.

En un sistema Ponzi nos encontramos que una persona (ya sea física o jurídica) ofrece gran rentabilidad a inversores, gracias a lo que consigue fácilmente convencer a la gente para que se le preste capital para ser invertido. Los intereses del dinero depositado o prestado son pagados con el dinero que invierten los nuevos clientes. Es decir, consiguen pagar los intereses de una inversión con el dinero de nuevas inversiones.

La rueda sigue funcionando hasta que deja de entrar dinero, y esto puede ser debido a una crisis, a que se acaben los estafados o a cualquier otro motivo. En ese momento, de desmonta el entramado que deja a los estafados sin el ahorro que habían invertido.

La captación se produce a través de anuncios en redes sociales donde se ofrece la posibilidad de obtener ingresos extras mediante la realización de tareas remotas. Estas publicidades dirigen a las víctimas a cuentas de WhatsApp o Telegram donde son atendidas por supuestos representantes de las compañías, quienes les indican que se registren en una plataforma para comenzar con sus tareas.

En un primer momento, las personas damnificadas no sospechan que se trata de una maniobra fraudulenta, pues ven, dentro de la plataforma, que se le reintegra el dinero que invirtieron y ven reflejadas las altas comisiones por las labores efectuadas. Sin embargo, no reparan en que los montos que transfieren son enviados a billeteras virtuales controladas por los propios estafadores.

En algunos casos, sólo pagan las primeras veces, liberando los fondos para que confíes, y vuelvas a invertir cada vez más.

Caso de Link Flow

Miles de personas en la región de Ayacucho acusaron una estafa por parte de esta organización al haber ingresado miles de soles en la tentadora propuesta de inversión digital.

Link Flow se trataba de una plataforma internacional que prometía ganancias fáciles siempre y cuando sus usuarios donaran dinero y, posteriormente, cumplieran con completar tareas tales como dar "me gusta", seguir y compartir publicaciones a través de las redes sociales.

Se podía acceder a sus beneficios mediante diferentes modalidades y así formar parte de la empresa con membresías que fueron denominadas VIP. Para ello, los suscriptores debían hacer aportes económicos y, mientras mayor era la inversión, Link Flow les ofrecía hasta triplicar la suma, pero en criptomonedas.

- VIP 2 PLUS = S/666 = 5 tareas
- VIP 3 PLUS = S/1,515 = 9 tareas
- VIP 4 PLUS = S/3,450 = 15 tareas
- VIP 5 PLUS = S/7,770 = 25 tareas

- VIP 6 PLUS = S/17,760 = 37 tareas
- VIP 7 PLUS = S/38,850 = 62 tareas
- VIP 8 PLUS = S/85,100 = 115 tareas
- VIP 9 PLUS = S/185,000 = 225 tareas

Tras conocerse el cierre de Link Flow en Perú en Ayacucho y otras regiones, los involucrados se mostraron angustiados ante el temor de no poder recuperar sus inversiones.

Y ahora se está ofreciendo recuperar el dinero invertido en dicha plataforma, pero pidiendo un cobro para dicha gestión, siendo los mismos que siguen estafando a los mismos usuarios.

Hay otras plataformas que se promocionan en diferentes portales conocidos como Mercado Libre, en donde se ofrecen rentabilidad inmediata y alta como invertir en acciones de Amazon, BCP, bienes raíces, petróleo, etc.

La Superintendencia de Banca, Seguros y AFP (SBS), en salvaguarda de los intereses de los ciudadanos, advierte que vienen operando en el país diversos esquemas de captación de dinero sin contar con autorización de la SBS:

Jubeadsa L Y G Coorporativo SAC – 'Grupo Económico L&G'	hxxps://grupoeconomicolyg.com/ hxxps://www.facebook.com/GrupoLyGinversiones hxxps://www.instagram.com/grupoeconomicolyg/ hxxps://www.tiktok.com/@grupo_economicolyg
Empresa Linkflow S.A.C. –'Linkflow'	hxxps://linkflow.site/
Cooperativa de Servicios Especiales SolbanPeru – 'Cooperativa SolbanPerú'	hxxps://www.facebook.com/Solbanperu.Oficial/
Mi Banquito Señor de Qoyllur Rity EIRL	hxxps://www.facebook.com/profile.php?id=100076460142098&locale=es_LA
Cooperativa de Servicios Múltiples Cusco Imperial Ltda.	Regiones de Cusco y Puno
Cooperativa de Servicios Múltiples Confianza Perú	Regiones de Puno y Madre de Dios

3. RECOMENDACIONES:

- Revisar si la empresa de inversión está regulada por la SBS.
- No participar en ofertas demasiado beneficiosas que presente rendimientos excesivamente altos, como las que circulan por redes sociales o servicios de mensajería.
- Buscar información en línea sobre la reputación de las empresas y si, mínimamente, están registradas ante las autoridades competentes para ofrecer este tipo de servicios.
- Nunca efectuar aportes de dinero ni realizar transferencias sin haber verificado la legitimidad de la oferta.
- No brindar información personal ni bancaria a través de plataformas digitales ni telefónicamente.

Fuente de Información:	• hxxps://www.fiscales.gob.ar/ciberdelincuencia/alertan-sobre-una-maniobra-de-fraude-a-traves-de-plataformas-que-ofrecen-supuestas-oportunidades-laborales/ • hxxps://larepublica.pe/sociedad/2024/05/30/estafa-de-link-flow-en-peru-que-es-y-para-que-servia-plataforma-que-permitia-ganar-dinero-en-linea-link-flow-estafa-lrsd-447510 • hxxps://elpopular.pe/actualidad/noticias-peru/2024/05/29/link-flow-que-es-para-que-sirve-cuando-inicio-a-operar-en-peru-y-como-capturaba-a-sus-usuarios-702293 • hxxps://www.sbs.gob.pe/noticia/detallenoticia/idnoticia/3733 • Análisis propio de redes sociales y Ciberpatrullaje

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°202	Fecha: 02-09-2024
		Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el servicio DSP de múltiples productos de Qualcomm		
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 uso después de la liberación en el servicio DSP de Qualcomm. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código malicioso, obtener acceso no autorizado y generar una condición de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-33060 de tipo uso después de la liberación en múltiples productos de Qualcomm. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código malicioso, obtener acceso no autorizado y generar una condición de DoS. La vulnerabilidad se debe a una corrupción de memoria cuando dos subprocesos intentan mapear y desasignar un solo nodo simultáneamente.

A. Productos afectados:

- Múltiples productos de Qualcomm.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad.
- Monitorear los avisos de seguridad de Qualcomm para obtener actualizaciones e información sobre parches.
- Implementar controles de acceso sólidos y segmentación de red para limitar la exposición potencial.
- Mantener todos los productos Qualcomm actualizados con las últimas versiones de firmware o software disponibles.
- Considerar la posibilidad de deshabilitar funciones o servicios innecesarios en los productos afectados hasta que haya un parche disponible.
- Implementar un monitoreo y registros sólidos para detectar cualquier posible intento de explotación.

Fuente de Información:	• hxxp://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html • hxxps://git.codelinaro.org/clo/la/kernel/msm-5.4/-/commit/4056f87e3b347e0283234f56b9e9aaea681d1644 • hxxps://git.codelinaro.org/clo/la/platform/vendor/qcom/opensource/dsp-kernel/-/commit/358c828263b8864b79396a6f2d098a2fde07f3e0

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°202	Fecha: 02-09-2024 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en el complemento DN Popup de WordPress		
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 falsificación de solicitud entre sitios (CSRF) en el complemento DN Popup de WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto hacer que un administrador que haya iniciado sesión las cambie mediante un ataque CSRF.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2024-7690 de tipo CSRF, existe debido a que el complemento no tiene una verificación CSRF activada al actualizar sus configuraciones, lo que podría permitir a los atacantes hacer que un administrador que haya iniciado sesión las cambie a través de un ataque CSRF.

Esta vulnerabilidad se debe a la falta de comprobaciones de falsificación de solicitud entre sitios cuando se actualizan las configuraciones del complemento. Esta ausencia de verificación puede permitir a los atacantes explotar la vulnerabilidad, lo que permite realizar cambios no autorizados en la configuración del complemento.

A. Productos afectados:

- complemento DN Popup de WordPress hasta la versión 1.2.2.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión estable del plugin desde el repositorio oficial de WordPress o actualizando desde el panel de administración.
- Mantener todos los plugins y temas de WordPress actualizados para minimizar los riesgos de seguridad.

Fuente de Información:	• hxxps://wpscan.com/vulnerability/1f941d51-1eaf-424a-95b8-ccaa3fdd339b/ • hxxp://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-7690 • hxxps://wordpress.org/plugins/dn-popup/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°202	Fecha: 02-09-2024 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Operadores de ransomware BlackByte explotan vulnerabilidad en VMware ESXi		
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 tomado conocimiento que los operadores del ransomware "BlackByte" vienen explotando activamente una vulnerabilidad de severidad **ALTA** de tipo omisión de autenticación en VMware ESXi para comprometer la infraestructura central de las redes empresariales. La explotación exitosa de esta vulnerabilidad podría permitir a un actor de amenazas con suficientes permisos de Active Directory (AD) obtener acceso completo a un host ESXi previamente configurado para utilizar AD para la gestión de usuarios.

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-37085 de tipo omisión de autenticación, afecta a los hipervisores VMware ESXi, específicamente relacionada con su integración con Active Directory (AD). Esta vulnerabilidad permite que un actor malintencionado con suficientes permisos de AD obtenga acceso administrativo completo a un host ESXi configurado para la administración de usuarios de AD al recrear el grupo predeterminado "Administradores de ESX" después de que se haya eliminado de AD.

Investigadores de Microsoft han indicado que actores de amenaza de ransomware "BlackByte" están utilizando una vulnerabilidad en el hipervisor ESXi de VMware para llevar a cabo ataques de encriptación masiva. Esta vulnerabilidad permite a los atacantes tomar control de los entornos virtualizados, lo que facilita la propagación del ransomware y la encriptación de datos a gran escala.

Los atacantes explotan esta vulnerabilidad para comprometer los servidores y acceder a datos sensibles, causando interrupciones significativas en las operaciones de las organizaciones afectadas.

La técnica incluye la ejecución de los siguientes comandos, que tienen como resultado la creación de un grupo denominado «ESX Admins» en el dominio y la adición de un usuario al mismo:

- net group «ESX Admins» /domain /add
- net group «ESX Admins» username /domain /add

A. Productos afectados:

- VMware ESXi versión 7.0 y 8.0;
- VMware Cloud Foundation versión 4.X y 5.X.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad.
- Implementar soluciones alternativas recomendadas si no es posible realizar actualizaciones inmediatas, como modificar la configuración avanzada de ESXi para mejorar la seguridad.
- Evitar exponer servidores ESXi a Internet público para reducir el riesgo de explotación.

Fuente de Información:	• hxxps://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/?msockid=080b47d41bdc622a265754171a31632a • hxxps://knowledge.broadcom.com/external/article?legacyId=1025569 • hxxps://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505

Índice alfabético