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

129-2025-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°129	Fecha: 04-06-2025
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Estafadores usan logos de Petroperú y TV Perú para engañar con falsas compensaciones		
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:

Una nueva modalidad de estafa circula en redes sociales, donde delincuentes utilizan los logos de entidades estatales como Petroperú y TV Perú para inducir a decenas de personas a entregar información personal y realizar depósitos de dinero con el falso argumento de recibir compensaciones económicas.

Este tipo de contenidos ya había sido advertido por Petroperú en ocasiones anteriores, cuando la empresa negó rotundamente estar vinculada a estas campañas y advirtió que se trata de una estafa que busca aprovecharse de la confianza del público. En su momento, la petrolera estatal recalcó que su único portal web oficial es www[.]petroperu.com.pe, y que solo sus cuentas verificadas en redes sociales son canales legítimos de comunicación.

2. DETALLES:

Durante un recorrido de verificación por distintos portales informativos y enlaces publicitarios, se detectó nuevamente la presencia de anuncios que utilizan de forma indebida el nombre y logotipo de Petroperú para promocionar un supuesto programa de inversión que promete “ganancias potenciales” en corto plazo.

En este portal fraudulento, se invita al usuario a ganar dinero mediante una inversión mínima de 100 dólares, induciendo a completar un formulario con datos personales, como nombre, correo y número telefónico. Incluso se simula un cálculo de ganancias y se muestran íconos de tarjetas de crédito para aparentar legalidad.

Una vez que las víctimas ingresan sus datos personales, reciben llamadas donde los delincuentes concretan la estafa.

Estos anuncios, con diseño atractivo y lenguaje persuasivo, indican que quienes nacieron entre 1950 y 1991 pueden acceder a pagos del Estado.

El mismo esquema se repite utilizando el logo del canal del Estado, TV Perú.

Indicadores de Compromiso:

KUNAK Consulting, un proveedor de Consultoría en ciberseguridad, reportó la existencia de varios sitios web fraudulentos:

- hxxps://ug.harmonicquantumfield.com/ptprog
- hxxps://oca.vibrantvisionvaultvista.com/csxx
- hxxps://www.facebook.com/61570841399998/videos/1042214781178434/
- hxxps://www.facebook.com/100083044336853/videos/690002517149226/
- hxxps://www.facebook.com/61565779157940/posts/122151824582525971/
- hxxps://www.facebook.com/61576346186248/posts/122095535276878206/

- hxxps://www.facebook.com/61571586154646/videos/630855476624424/
- hxxps://www.facebook.com/61573997053283/videos/1917228719087155/
- hxxps://www.facebook.com/61575498785745/videos/1885608695508312/
- hxxps://www.facebook.com/61570841399998/videos/1349725226268830/
- hxxps://www.facebook.com/61570328580874/videos/4020321231576246/
- hxxps://www.facebook.com/61572615290505/videos/3974713706136447/
- hxxps://www.facebook.com/61551469212836/videos/1030305618995225/

3. RECOMENDACIONES:

- Extremar precauciones con cualquier página que solicite dinero o información personal a nombre de entidades públicas sin pasar por canales oficiales.
- No interactuar con las personas y las redes sociales que vienen presentando este tipo de publicaciones, que buscan un beneficio económico.
- Educar a los usuarios sobre cómo reconocer los intentos de phishing.
- Denunciar estos casos ante las autoridades competentes como a la PNP y Ministerio Público.

Fuente de Información:	• hxxps://panamericana.pe/24horas/locales/444527-estafadores-logos-petroperu-tv-peru-enganar-falsas-compensaciones • hxxps://elgasnoticias.com/siguen-usando-nombre-y-logotipo-de-petroperu-para-promover-falsos-programas-de-inversion-en-portales-digitales/ • hxxps://www.petroperu.com.pe/petroperu-advierte-de-estafas-sobre-falso-programa-de-inversion

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°129	Fecha: 04-06-2025 Página: 6 de 8

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

Schneider Electric ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo desbordamiento de búfer clásico que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado inyectar código o eludir la autenticación.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2023-4041 de tipo desbordamiento de búfer clásico que afecta a varios de sus productos, podría permitir a un atacante remoto no autenticado inyectar código o eludir la autenticación.

La vulnerabilidad de desbordamiento de búfer clásico, escritura fuera de límites y descarga de código sin comprobación de integridad en el gestor de arranque Gecko de Silicon Labs en ARM (módulos del analizador de archivos de actualización de firmware) que permite la inyección de código y la omisión de la autenticación. Este problema afecta a las versiones "autónoma" y "de aplicación" del gestor de arranque Gecko.

A. Productos afectados:

- Wiser AvatarOn 6K Freelocate: Todas las versiones.
- Zócalo Wiser Cuadro H 5P: Todas las versiones.

3. RECOMENDACIÓN:

- Desactivar inmediatamente la actualización de firmware en el Centro de Confianza de Zigbee o retirar los productos del servicio para reducir el riesgo de explotación, ya que los productos Wiser AvatarOn 6K Freelocate y Wiser Cuadro H 5P Socket han llegado al final de su vida útil y ya no reciben soporte.

.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-153-01 • hxxps://www.se.com/en/work/support/cybersecurity/securitynotifications.jsp

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°129	Fecha: 04-06-2025 Página: 7 de 8

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

Cisco Systems, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo uso de contraseñas codificadas en las implementaciones en la nube de Cisco Identity Services Engine (ISE) de Amazon Web Services (AWS), Microsoft Azure y Oracle Cloud Infrastructure (OCI). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado acceder a datos confidenciales, ejecutar operaciones administrativas limitadas, modificar configuraciones del sistema e interrumpir servicios dentro de los sistemas afectados.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-20286 de tipo uso de contraseñas codificadas en las implementaciones en la nube de Cisco ISE de AWS, Microsoft Azure y OCI, podría permitir a un atacante remoto no autenticado acceder a datos confidenciales, ejecutar operaciones administrativas limitadas, modificar configuraciones del sistema e interrumpir servicios dentro de los sistemas afectados.

Esta vulnerabilidad existe porque las credenciales se generan incorrectamente al implementar Cisco ISE en plataformas en la nube, lo que provoca que diferentes implementaciones de Cisco ISE compartan las mismas credenciales. Estas credenciales se comparten entre múltiples implementaciones de Cisco ISE siempre que la versión de software y la plataforma en la nube sean las mismas. Un atacante podría explotar esta vulnerabilidad extrayendo las credenciales de usuario de Cisco ISE implementado en la nube y usándolas para acceder a Cisco ISE implementado en otros entornos de nube a través de puertos no seguros. Una explotación exitosa podría permitir al atacante acceder a datos confidenciales, ejecutar operaciones administrativas limitadas, modificar la configuración del sistema o interrumpir los servicios de los sistemas afectados.

Si el nodo de administración principal está implementado en la nube, Cisco ISE se ve afectado por esta vulnerabilidad. Si el nodo de administración principal está implementado localmente, no se ve afectado.

A. Productos afectados:

- Cisco Identity Services Engine (ISE) de Amazon Web Services (AWS), versión 3.1, 3.2, 3.3 y 3.4.
- Microsoft Azure, versión 3.2, 3.3 y 3.4.
- Oracle Cloud Infrastructure (OCI), versión 3.2, 3.3 y 3.4.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-aws-static-cred-FPMjUcm7

Índice alfabético