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

105-2024-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°105	Fecha: 06-05-2024
		Página: 4 de 6

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Cuidado con los Ataques de Phishing dirigidos a usuarios de Tarjetas AmericanExpress		
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:

Los ciberdelincuentes se dirigen a los titulares de tarjetas American Express a través de correos electrónicos engañosos que imitan las comunicaciones oficiales del gigante de los servicios financieros.

2. DETALLES:

Según un tweet reciente de Avast Threat Labs, el ataque de phishing comienza con un correo electrónico que parece ser de American Express instando a los destinatarios a participar en un proceso de configuración falso de una "Clave de seguridad personal de American Express".

Estos correos electrónicos pretenden alertar a los destinatarios sobre una supuesta "verificación de seguridad crítica", instándolos a actualizar los detalles de su cuenta American Express de inmediato. El objetivo principal de estos correos electrónicos de phishing es engañar a los destinatarios para que revelen sus credenciales de inicio de sesión.

El correo electrónico contiene un enlace que dirige a los usuarios a una página web fraudulenta alojada en plataformas como Google Forms.

A las víctimas se les pide que ingresen su número de seguro social, fecha de nacimiento, apellido de soltera de la madre, dirección de correo electrónico y detalles completos de su tarjeta American Express, incluidos los códigos de seguridad y la fecha de vencimiento.

El diseño y el lenguaje del correo electrónico y la página web imitan fielmente las comunicaciones legítimas de American Express, lo que hace que la estafa sea particularmente convincente.

American Express aconseja a los clientes que estén atentos e informen inmediatamente de actividades sospechosas.

3. RECOMENDACIONES:

- Verificar la dirección de correo electrónico del remitente.
- Buscar errores ortográficos sutiles o dominios incorrectos que puedan indicar un intento de phishing.
- Buscar saludos genéricos. Los correos electrónicos de phishing suelen utilizar saludos genéricos como "Estimado cliente" en lugar de su nombre.
- No hacer clic en enlaces sospechosos o no solicitados. En su lugar, visitar el sitio web escribiendo la dirección directamente en su navegador.
- Comunicarse directamente con la empresa, si recibe una solicitud inesperada de información personal, utilizando un número de teléfono o una dirección de correo electrónico desde su sitio web oficial.
- Utilizar software de seguridad. Proteger sus dispositivos con software antivirus actualizado, que puede ayudar a detectar y bloquear descargas y sitios maliciosos.
- Diseñar una estrategia de concientización y capacitación que incluya la responsabilidad en el manejo de la información. Realizar capacitaciones periódicas para dos grupos: los usuarios finales y su equipo de seguridad.

Fuente de Información:	• hxxps://gbhackers.com/beware-of-phishing-attacks/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°105	Fecha: 06-05-2024 Página: 5 de 6

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades de escritura fuera de los límites en Development System de CODESYS		
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 **ALTA** de tipo escritura fuera de los límites y usar después gratis en Development System de CODESYS. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario o bloquear el sistema debido a una vulnerabilidad de escritura fuera de límites.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-49675 de tipo escritura fuera de los límites que afecta a la herramienta de programación IEC 61131-3, podría permitir a un atacante local no autenticado engañar a un usuario para que abra archivos de proyecto corruptos para ejecutar código arbitrario o bloquear el sistema debido a una vulnerabilidad de escritura fuera de límites.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-49676 de tipo usar después gratis, podría permitir a un atacante local no autenticado engañar a un usuario para que abra archivos de proyecto corruptos y bloquear el sistema debido a una vulnerabilidad de uso posterior a la liberación.

A. Productos afectados:

- CODESYS Development System, versiones anteriores a 2.3.9.73.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://cert.vde.com/de/advisories/VDE-2024-024/

Índice alfabético