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

070-2025-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°070	Fecha: 25-03-2025
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	La estafa de la vinculación de las Cuentas Bancarias con Billeteras Digitales		
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:

Un nuevo tipo de fraude digital está en ascenso, los delincuentes están logrando transferir tarjetas bancarias de sus víctimas a billeteras digitales en sus propios dispositivos móviles, lo que les permite realizar compras sin restricciones y con menos probabilidades de ser detectados de inmediato.

2. DETALLES:

El fraude comienza con un engaño inicial que busca obtener los datos de la víctima, utilizando para ello métodos de phishing, como mensajes de texto que suplantan a algún organismo fiable, avisos falsos de recompensas o de multas de tránsito, publicidad engañosa sobre ventas de liquidación por parte de marcas reconocidas, etc.

En todos los casos anteriores, existe algún tipo de inminente limitación temporal antes de que el usuario se vea obligado a perder una oportunidad o a tener que pagar más, lo que genera sensación de urgencia en la víctima.

El paso más importante del engaño ocurre cuando el delincuente solicita al banco un código de autenticación (OTP) para registrar la tarjeta de la víctima en su propia billetera digital.

Un código OTP es una contraseña de un único uso (One-Time Password), que tiene como fin evitar el fraude en gestiones y trámites digitales identificando de manera inequívoca a una determinada persona. Este código OTP tiene una única validez, por lo que no es reutilizable. Es un método muy seguro y su tiempo de validez es limitado.

Al introducir los datos en el sitio fraudulento, la víctima recibe un mensaje real de su banco con un código OTP. Sin darse cuenta de la trampa, la víctima proporciona este código a los estafadores, creyendo que es parte del proceso de pago.

Los delincuentes usan este código para autorizar la vinculación de la tarjeta en sus propios teléfonos mediante billeteras digitales como Apple Pay, Google Wallet o Samsung Pay.

Con el fraude completado, el estafador puede hacer compras online, pagos en tiendas físicas, adquisición de tarjetas de regalo, etc. Incluso, Los teléfonos con tarjetas robadas pueden ser vendidos a otros delincuentes, creando un mercado negro donde estas cuentas son reutilizadas para más fraudes.

Muchas veces esperan hasta tres meses antes de comenzar a gastar, lo que reduce las probabilidades de que el banco detecte actividades sospechosas.

3. RECOMENDACIONES:

- No compartir nunca códigos OTP ni cualquier código que se reciba bajo ninguna circunstancia, ni siquiera a supuestos empleados bancarios.
- Desconfiar de ofertas demasiado buenas para ser verdad
- Configurar alertas en la aplicación del banco para recibir notificaciones inmediatas de cualquier movimiento en la cuenta, y denunciarlo al banco o a las autoridades pertinentes.

Fuente de Información:	• hxxps://www.genbeta.com/seguridad/cuando-estafador-lleva-tu-dinero-su-movil-timo-que-cada-vez-preocupa-a-expertos • hxxps://firmafy.com/codigo-otp-que-es-y-como-funciona/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°070	Fecha: 25-03-2025 Página: 5 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en componente de Scheneider Electric SE		
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:

Scheneider Electric SE ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo inicialización predeterminada insegura de un recurso que afecta al componente WebHMI de Schneider Electric, que forma parte de las soluciones EcoStruxure Power Automation System y EcoStruxure Microgrid Operation Large (EMO-L). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar comandos no autorizados y provocar graves interrupciones en las operaciones industriales.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-1960 de tipo inicialización predeterminada insegura de un recurso que afecta al componente WebHMI de Schneider Electric, podría permitir a un atacante remoto modificar archivos o denegar el acceso a recursos sin interacción del usuario.

Existe una vulnerabilidad de inicialización de un recurso con un valor predeterminado inseguro que podría provocar que un atacante ejecute comandos no autorizados cuando las credenciales de contraseña predeterminadas de un sistema no se hayan cambiado en el primer uso. El nombre de usuario predeterminado no se muestra correctamente en la interfaz WebHMI.

La vulnerabilidad surge del uso de credenciales predeterminadas inseguras que permanecen inalteradas la primera vez que se usan. La interfaz WebHMI no muestra correctamente el nombre de usuario predeterminado, lo que aumenta la probabilidad de que las organizaciones pasen por alto el cambio de estas credenciales. Este descuido puede permitir a los atacantes ejecutar comandos no autorizados y, potencialmente, obtener el control total del sistema afectado.

A. Productos afectados:

- WebHMI v4.1.0.0 y anteriores, implementado con la interfaz de usuario del sistema de automatización de energía EcoStruxure (EPAS) v2.6.30.19 y anteriores.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad. Schneider Electric ha proporcionado una corrección, WebHMI_Fix_users_for_Standard.V1, para solucionar esta vulnerabilidad.
- Implementar todas las pautas de endurecimiento proporcionadas con el producto.
- Asegurarse de que WebHMI no esté expuesto a Internet.
- Seguir las mejores prácticas generales de ciberseguridad, como aislar los sistemas de control detrás de firewalls y utilizar métodos de acceso remoto seguro como VPN.

Fuente de Información:	• hxxps[:]//download[.]schneider-electric[.]com/files?p_Doc_Ref=SEVD-2025-070-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-070-03.pdf

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°070	Fecha: 25-03-2025
		Página: 6 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de código en Microsoft Edge		
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 Corporation ha publicado una vulnerabilidad de severidad **MEDIA** de tipo ejecución remota de código (RCE) que afecta a la versión de Microsoft Edge basada en Chromium. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario y comprometer el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-29806 de tipo ejecución remota de código (RCE), podría a un atacante remoto ejecutar código arbitrario y comprometer el sistema afectado.

Esta vulnerabilidad permite a atacantes no autorizados ejecutar código arbitrario en una red incitando a los usuarios a visitar páginas web maliciosas. Un atacante remoto puede engañar a la víctima para que haga clic en una URL especialmente diseñada y ejecutar código arbitrario en el sistema.

A. Productos afectados:

- Microsoft Edge (basado en Chromium) versiones anteriores a 129.0.2792.52.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad. Los usuarios y administradores deben actualizar Microsoft Edge a la última versión estable para protegerse contra posibles vulnerabilidades.

Fuente de Información:	• hxxps[:]//msrc[.]Microsoft[.]com/update-guide/vulnerability/CVE-2025-29806

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°070	Fecha: 25-03-2025 Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en la biblioteca “libxslt” de Red Hat Enterprise Linux		
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:

Red Hat Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo uso después de la liberación (use after-free) que afecta a la biblioteca “libxslt” de Red Hat Enterprise Linux. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante modificar archivos o denegar el acceso a recursos sin interacción del usuario.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-24855 de tipo uso después de la liberación, podría permitir a un atacante modificar archivos o denegar el acceso a recursos sin interacción del usuario.

Esta vulnerabilidad surge de evaluaciones XPath anidadas donde un nodo de contexto XPath se modifica, pero no se restaura, lo que provoca problemas de corrupción de memoria e involucra funciones como xsltNumberFormatGetValue, xsltEvalXPathPredicate, xsltEvalXPathStringNs y xsltComputeSortResultInternal.

La vulnerabilidad no requiere la interacción del usuario y puede explotarse sin acceder a la configuración ni a los archivos del sistema vulnerable. Sin embargo, su nivel de explotabilidad es relativamente bajo, lo que indica que su explotación podría ser difícil.

A. Productos afectados:

- Red Hat Enterprise Linux para ARM 64: 9.
- Red Hat Enterprise Linux para Power, little endian: 9.
- Red Hat Enterprise Linux para IBM z Systems: 9.
- Red Hat Enterprise Linux para x86_64: 9.
- libxslt (paquete Red Hat): anterior a 1.1.34-9.el9_5.1.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Actualizar Microsoft Edge a la última versión estable para protegerse contra posibles vulnerabilidades.

Fuente de Información:	• hxxps[:]//Access[.]redhat[.]com/errata/RHSA-2025:3107 • hxxps[:]//gitlab[.]gnome[.]org/GNOME/libxslt/-/issues/128

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°070	Fecha: 25-03-2025
		Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el controlador NGINX para Kubernetes		
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 Corporation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo ejecución de código de configuración de NGINX asociadas con el problema "IngressNightmare" que afecta al controlador Ingress NGINX en Azure Kubernetes Service (AKS). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado comprometer la seguridad de los recursos de Ingress, esenciales para gestionar el acceso externo a los servicios dentro de un clúster de Kubernetes.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-1974 de tipo ejecución de código asociadas con el problema "IngressNightmare" que afecta al controlador Ingress NGINX en AKS, podría permitir a un atacante remoto no autenticado comprometer la seguridad de los recursos de Ingress, esenciales para gestionar el acceso externo a los servicios dentro de un clúster de Kubernetes,

Esta vulnerabilidad implica la ejecución de código de configuración de NGINX, lo que permite a los atacantes ejecutar código arbitrario en el pod del controlador Ingress NGINX. La explotación de esta vulnerabilidad, junto con otras vulnerabilidades de inyección relacionadas, puede provocar la ejecución remota no autorizada de código sin autenticación, lo que podría permitir el control total de un clúster de Kubernetes.

La explotación puede dar como resultado la toma de control del clúster, lo que permite el acceso a todos los secretos en los espacios de nombres y potencialmente conduce a la exposición de datos confidenciales.

A. Productos afectados:

- Controlador Ingress NGINX para Kubernetes, múltiples versiones.

3. RECOMENDACIONES:

- Actualizar a versiones parcheadas del controlador Ingress NGINX (versiones 1.12.1, 1.11.5 y 1.10.7) y verificar que el punto final del webhook de admisión no esté expuesto externamente.
- Limitar solo el acceso del servidor API de Kubernetes al controlador de admisión y deshabilitar temporalmente el componente del controlador de admisión si no es necesario.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-1974 • hxxps://www.hendryadrian.com/critical-ingress-nginx-controller-vulnerability-allows-rce-without-authentication/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°070	Fecha: 25-03-2025 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Simcenter Femap de Siemens		
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 Corporation ha publicado una vulnerabilidad de severidad **ALTA** de tipo restricción inadecuada de operaciones dentro de los límites de un búfer de memoria que afecta a Simcenter Femap de Siemens. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código dentro del proceso actual del producto.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-25175 de tipo restricción inadecuada de operaciones dentro de los límites de un búfer de memoria que afecta a Simcenter Femap de Siemens, podría permitir a un atacante remoto no autenticado ejecutar código dentro del proceso actual del producto.

Siemens Simcenter Femap presenta una vulnerabilidad de corrupción de memoria al analizar archivos .NEU especialmente diseñados. Esto podría permitir que un atacante ejecute código en el contexto del proceso actual.

A. Productos afectados:

- Simcenter Femap V2401: Versiones anteriores a V2401.0003.
- Simcenter Femap V2406: Versiones anteriores a V2406.0002.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad.
- No abrir archivos NEU que no sean de confianza en la aplicación afectada, para todos los productos afectados.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-079-03

Índice alfabético