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

095-2025-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°095	Fecha: 23-04-2025
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	La mayoría de los ataques phishing parecen de día cero por sus elevadas capacidades para evadir la detección		
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

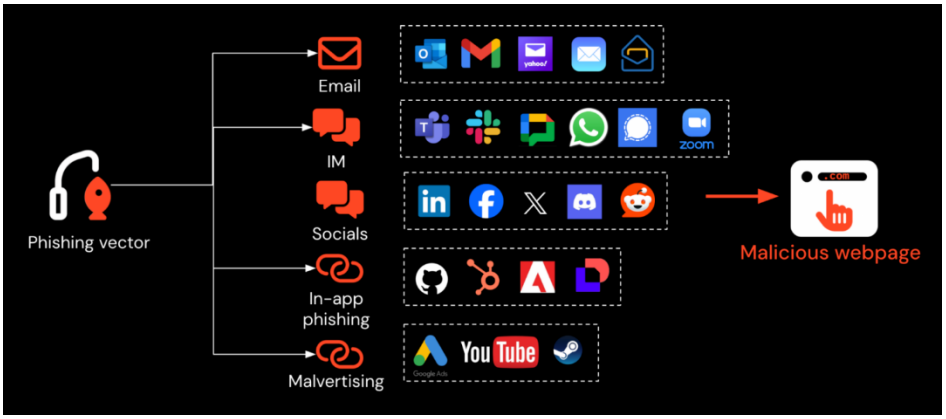
1. ANTECEDENTES:

Los ataques de phishing seguirán siendo un gran desafío para las organizaciones en 2025. De hecho, dado que los atacantes utilizan cada vez más técnicas basadas en la identidad en lugar de exploits de software, se podría decir que el phishing representa una amenaza mayor que nunca.

Con los kits de phishing que eluden la MFA como nueva norma, capaces de phishing en cuentas protegidas por SMS, OTP y métodos push, los controles de detección se encuentran bajo presión constante mientras que los controles de prevención fallan.

2. DETALLES:

La mayoría de los ataques de phishing implican el envío de un enlace malicioso al usuario, el cual, al acceder, carga una página maliciosa. En la gran mayoría de los casos, la página maliciosa es un portal de inicio de sesión para un sitio web específico, donde el objetivo del atacante es robar la cuenta de la víctima.



La detección de phishing se basa, en esencia, en listas negras compuestas por indicadores de compromiso (IoC) relacionados con páginas de phishing identificadas con éxito como maliciosas. Estos IoC consisten en dominios, URL e IP maliciosos que han aparecido en un ataque.

Los proveedores de seguridad y de servicios recopilan los IoC de diversas fuentes. Pero esto significa que una posible víctima debe interactuar con ella de alguna manera, ya sea cayendo en un ataque de phishing o reportándola como sospechosa. Si se puede acceder a la página y analizarla, y se encuentra contenido malicioso se pueden recopilar los indicadores de compromiso de la página y añadirlos a una lista de bloqueo.

Esta información comenzará a circular a través de las diversas fuentes de inteligencia de amenazas y productos de seguridad que la aprovechan.

La mayor parte de la detección y el control del phishing se centran en la capa de correo electrónico y red, generalmente en la Puerta de Enlace de Correo Electrónico Seguro (SEG), la Puerta de Enlace Web Segura (SWG)/proxy, o ambas.

Los dominios de phishing son, por naturaleza, altamente desechables. Los atacantes los compran al por mayor, usurpando constantemente dominios legítimos y, por lo general, previendo que se les escapará una gran cantidad.

La arquitectura moderna de phishing también puede rotar y actualizar dinámicamente elementos comúnmente firmados; por ejemplo, rotando dinámicamente los enlaces servidos a los visitantes desde un grupo continuamente actualizado (de modo que cada persona que hace clic en el enlace recibe una URL diferente) e incluso llegando al punto de usar cosas como enlaces mágicos de un solo uso (lo que también significa que cualquier miembro del equipo de seguridad que intente investigar la página más tarde no podrá hacerlo). Si un dominio se marca como malicioso, el atacante solo tiene que registrar un nuevo dominio o comprometer un servidor WordPress en un dominio ya confiable. Ambas cosas están sucediendo a gran escala, ya que los atacantes se preparan para el riesgo de que sus dominios sean destruidos en algún momento.

Tanto las soluciones basadas en correo electrónico como en red (proxy) dependen de la capacidad de inspeccionar y analizar una página para identificar si es maliciosa o no, después de lo cual se generan IoC que se pueden aplicar cuando se hace clic en un enlace.

Las páginas de phishing son ahora aplicaciones web dinámicas, por lo que la mayoría de las comprobaciones estáticas básicas no logran identificar el contenido malicioso que se ejecuta en la página.

Incluso para un entorno de pruebas, los atacantes simplemente implementan protección contra bots, requiriendo la interacción del usuario con un CAPTCHA. También están ofuscando elementos visuales y DOM para evitar que las detecciones basadas en firmas los detecten, por lo que incluso si puede llegar a la página, hay una gran probabilidad de que sus detecciones no se activen.

Por ejemplo, un atacante piratea un blog de WordPress para obtener un dominio confiable y luego ejecuta un kit de herramientas de phishing en la página web. Envía un enlace a uno de sus empleados por correo electrónico. Su solución de escaneo de correo electrónico lo inspecciona en un entorno de pruebas, pero el kit de phishing lo detecta y redirige a un sitio web seguro para que supere la inspección.

El usuario recibe el correo electrónico con el enlace y ya puede interactuar con la página de phishing. Introduce sus credenciales y el código MFA en la página, con lo cual el atacante roba la sesión autenticada y se hace con el control de la cuenta del usuario.

Para detener los ataques de phishing en el momento en que ocurren, necesitamos poder observar la página en tiempo real, tal como la ve el usuario desde el navegador. No en un entorno aislado, sino viendo la página real al mismo tiempo que el usuario.

3. RECOMENDACIONES:

- Implementar una solución de seguridad de identidad basada en navegador que intercepta los ataques de phishing en el momento en que ocurren, en los navegadores de los empleados., de tal manera que bloquee al usuario y no pueda interactuar con el sitio de phishing.
- Implementar controles en tiempo real que se activan cuando se detecta un elemento malicioso.
- Usar una solución que brinde capacidades integrales de detección y respuesta ante ataques de identidad contra técnicas como el robo de credenciales, la pulverización de contraseñas y el secuestro de sesiones mediante tokens de sesión robados.
- Detectar y corregir vulnerabilidades de identidad en todas las aplicaciones que usan sus empleados, como inicios de sesión fantasma, brechas de cobertura de SSO, brechas de MFA, y contraseñas débiles, vulneradas y reutilizadas.
- No abrir archivos adjuntos ni enlaces presentes en correos electrónicos sospechosos ni en otros mensajes.
- Descargar sólo desde sitios oficiales. Siempre verificar la autenticidad del sitio web.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Realizar análisis regulares del sistema para eliminar amenazas persistentes.
- Educar a los usuarios sobre cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/phishing-detection-is-broken-why-most-attacks-feel-like-a-zero-day/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°095	Fecha: 23-04-2025 Página: 6 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en NVIDIA NeMo Framework		
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:

Nvidia Corporation ha publicado una vulnerabilidad de severidad **ALTA** de tipo deserialización de datos no confiables que afecta a NVIDIA NeMo Framework. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución de código arbitrario.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-23249 de tipo deserialización de datos no confiables, podría permitir a un atacante ejecutar código arbitrario de forma remota, lo que supone importantes riesgos de seguridad.

Esta vulnerabilidad representa un riesgo significativo para la privacidad de los usuarios, ya que permite el acceso no autorizado a información personal y la posibilidad de realizar acciones maliciosas que comprometan su seguridad y confidencialidad.

A. Productos afectados:

- NVIDIA Nemo Framework: versión 25.02 y anteriores.

3. RECOMENDACIÓN:

- Aplicar los últimos parches de seguridad de NVIDIA para NeMo Framework.

Fuente de Información:	• hxxps[:]//nvidia[.]custhelp[.]com/app/answers/detail/a_id/5641

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°095	Fecha: 23-04-2025 Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Mitsubishi Electric Europe BV smartRTU		
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:

Mitsubishi Electric ha publicado una vulnerabilidad de severidad **ALTA** de tipo inyección de comandos del sistema operativo que afecta a los dispositivos Mitsubishi Electric smartRTU. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto eludir la autenticación y ejecutar comandos arbitrarios del sistema operativo en el dispositivo.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-3128 de tipo inyección de comandos del sistema operativo, podría permitir a un atacante remoto eludir la autenticación y ejecutar comandos arbitrarios del sistema operativo en el dispositivo.

Un atacante que logre eludir la autenticación, explotando una vulnerabilidad de elusión de autenticación relacionada (CVE-2025-3232), puede usar una ruta API específica para inyectar y ejecutar comandos arbitrarios del sistema operativo en el dispositivo smartRTU 5. Su explotación exitosa puede resultar en la divulgación, manipulación destrucción de datos, eliminación de archivos o componentes del sistema y generar una condición de denegación de servicio (DoS) en el dispositivo afectado.

CVE-2025-3232 es una vulnerabilidad relacionada que implica una evasión de autenticación y que se puede utilizar junto con CVE-2025-3128 para facilitar su explotación.

A. Productos afectados:

- Mitsubishi Electric Europe BV smartRTU: Versiones 3.37 y anteriores.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Utilizar un firewall o VPN para restringir el acceso no autorizado a Internet.
- Operar el dispositivo estrictamente dentro de una LAN confiable.
- Bloquear el acceso desde redes y hosts que no sean confiables mediante firewalls.
- Implementar un firewall de aplicaciones web (WAF) para filtrar, monitorear y bloquear el tráfico HTTP/HTTPS malicioso.
- Permitir el acceso de clientes web sólo desde redes confiables.
- Supervisar el tráfico de la red para detectar actividad sospechosa y revise los registros de acceso periódicamente.

Fuente de Información:	• hxxps[:]//eu-assets[.]contentstack[.]com/v3/assets/blt5412ff9af9aef77f/blte89b2dd6dc6048fc/MEU_PSIRT_2025-3128

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°095	Fecha: 23-04-2025 Página: 8 de 10

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

Tenable ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo error de validación de entrada en el componente de PostgreSQL para Security Center. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar consultas SQL arbitrarias en la base de datos.

2. DETALLES:

Tenable Security Center es una plataforma robusta de gestión de vulnerabilidades basada en riesgos que permite a las organizaciones descubrir, evaluar y priorizar vulnerabilidades en toda su infraestructura de TI. Sus análisis avanzados, flujos de trabajo personalizables y capacidades de integración lo convierten en la opción preferida para las organizaciones que buscan información práctica y control sobre su riesgo cibernético, especialmente en entornos que requieren gestión de datos local.

Tenable Security Center utiliza software de terceros para proporcionar la funcionalidad subyacente. Se detectó que uno de los componentes de terceros (PostgreSQL) contenía vulnerabilidades, y el proveedor ha publicado versiones actualizadas.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-1094 de tipo error de validación de entrada en el componente de PostgreSQL para Security Center, podría permitir a un atacante remoto ejecutar consultas SQL arbitrarias en la base de datos.

La vulnerabilidad existe debido a una validación insuficiente de la sintaxis de comillas en las funciones PQescapeLiteral(), PQescapeIdentifier(), PQescapeString() y PQescapeStringConn() de libpq de PostgreSQL, así como en las utilidades de línea de comandos cuando client_encoding es BIG5 y server_encoding es EUC_TW o MULE_INTERNAL. Un atacante remoto puede pasar una entrada especialmente diseñada a la aplicación y ejecutar consultas SQL arbitrarias en la base de datos. Esta vulnerabilidad está siendo explotado activamente en la naturaleza.

A. Producto afectado:

- SecurityCenter: SC-202310.1 - 6.5.1.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que abordan esta vulnerabilidad.

Fuente de Información:	• hxxps://www.tenable.com/security/tns-2025-06 • hxxps://www.tenable.com/cve/CVE-2025-1094

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°095	Fecha: 23-04-2025 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de escritura fuera de límites en productos 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 SE ha publicado una vulnerabilidad de severidad **ALTA** de tipo escritura fuera de límites 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 objetivo.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-37036 de tipo escritura fuera de límites en múltiples productos de Schneider Electric, podría permitir que un atacante remoto comprometa el sistema vulnerable.

La vulnerabilidad existe debido a un error de límite al procesar entradas no confiables. Un atacante remoto puede enviar una solicitud POST especialmente diseñada, activar una escritura fuera de límites y ejecutar código arbitrario en el sistema objetivo.

A. Productos afectados:

- Sage 1410: C3414-500-S02K5_P8.
- Sage 1430: C3414-500-S02K5_P8.
- Sage 1450: C3414-500-S02K5_P8.
- Sage 2400: C3414-500-S02K5_P8.
- Sage 4400: C3414-500-S02K5_P8.
- Sage 3030 Magnum: C3414-500-S02K5_P8.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.

Fuente de Información:	• hxxps://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-163-05&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-163-05.pdf

Índice alfabético