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

123-2025-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

Correo phishing con Resolución judicial fraudulenta 4
Vulnerabilidad de severidad crítica en la pila Bluetooth de Apache NuttX RTOS 7
Vulnerabilidad en la herramienta de configuración iSTAR (ICU) de Johnson Controls 8
Vulnerabilidad de ejecución remota de código en el kit de herramientas NVIDIA CUDA 9
Índice alfabético 10

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°123	Fecha: 27-05-2025
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Correo phishing con Resolución judicial fraudulenta		
Tipo de Ataque	Suplantación	Abreviatura	Suplantación
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:

La suplantación es un término general para definir el enmascaramiento de un ciberdelincuente, que se hace pasar por una entidad o dispositivo de confianza para que hagas algo que beneficia al atacante y te perjudica.

2. DETALLES:

Se está detectando la recepción de un correo electrónico sospechoso proveniente de la dirección pnp.04.gob.pe@alertiservice.com, que contiene amenazas legales y un archivo adjunto PDF simulando una resolución judicial de la Policía Nacional del Perú (PNP). El contenido está diseñado para intimidar al receptor y se clasifica como un intento de phishing y extorsión digital.

El asunto del correo indica "RESOLUCIÓN JUDICIAL DIRECTA" y lleva un adjunto en pdf que incluye amenazas legales e información falsa.

Policía Nacional Del Perú
Dirección De Investigación De Ciberdelincuencia
Dirección De Protección Del Menor
Av. Canaval Y Moreyra Cdra. 6 - San Isidro - Lima - Lima - Perú
(Referencia: Plaza 30 De Agosto S/N)

Mayo 2025

A la atención de la presunta víctima,

La Policía Nacional del Perú, en colaboración con Interpol, ha iniciado un procedimiento judicial en forma de orden judicial inmediata contra su dirección de Protocolo de Internet (IP). Esta acción ha sido tomada bajo la autoridad del Comandanté Général de la Policía, Sr. Víctor José Zanabria Angula, en respuesta a la visualización y posesión de material que muestra a menores de edad participando en conductas sexualmente explícitas.

La demostración se llevó a cabo utilizando un proceso de rastreo forense anti-python de alta tecnología, que ha demostrado ser capaz de capturar a los usuarios de Internet que visitan los sitios web prohibidos.

Se ha comprobado que este proceso rastrea a los usuarios de Internet que acceden a sitios web prohibidos que contienen pornografía juvenil, sin dejar rastro digital. También abarca la adquisición y el procesamiento de imágenes digitales, el cálculo de valores hash, la recuperación de datos borrados de discos duros, los últimos sistemas operativos de teléfonos móviles (Android, IOS y chino), servidores y herramientas forenses portátiles para su examen in situ.

La ley establece que: -
(1) Toda persona que prepare, produzca o exhiba cualquier tipo de pornografía infantil, ya sea para sí misma o para su publicación, será culpable de un delito y podrá ser condenada a penas de prisión.

(2) Toda persona que reciba, difunda, distribuya o venda pornografía infantil será culpable de un delito punible con pena de prisión.
B: Toda persona que intencionadamente provoque o incite a una persona menor de dieciocho años a participar en pornografía infantil será culpable de un delito punible con pena de prisión.

Esta comunicación se basó en el resultado del rastreo de su dirección IP utilizada para acceder a contenidos en línea relacionados con estos sitios web, lo que comúnmente se denomina «rastreo».

Se ruega que envíe una respuesta en un plazo de 24 horas a partir de la recepción de esta comunicación para recibir instrucciones adicionales. La falta de respuesta en este plazo puede dar lugar al inicio de acciones legales inmediatas.

Se le advierte

Observatorio Peruano de Cibercriminalidad

Víctor José Zanabria Angulo
Comandante General De La Policía Nacional Del Perú

El dominio alertiservice.com presenta un servicio HTTP activo que responde con el código HTTP 423 (Locked), indicando que el recurso solicitado está restringido y requiere autenticación o condiciones específicas de acceso.

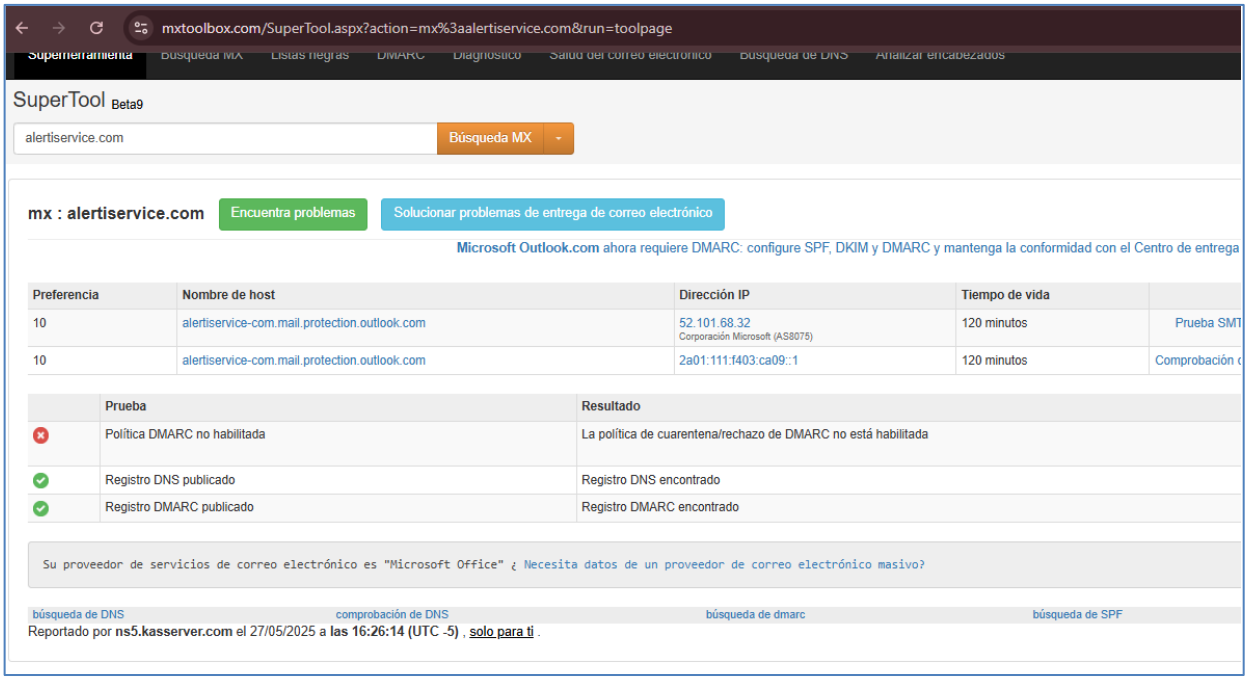
Su estado actual es clientTransferProhibited y su expiración está prevista para el 26 de diciembre de 2025. No se identifican datos del propietario, pero el contacto de abuso es abuse@registrygate.com. Estos elementos, combinados, refuerzan su clasificación como dominio sospechoso usado con fines maliciosos.

Este comportamiento confirma que:

- El servidor web está activo y operativo.
- El contenido está intencionalmente oculto o protegido.
- La infraestructura fue probablemente configurada para evadir detección y facilitar acciones encubiertas, como campañas de phishing o carga de comandos.

La respuesta HTTP 423 refuerza la hipótesis de uso malicioso, al no exponer contenido público y operar bajo una lógica de acceso cerrado.

El dominio alertiservice.com cuenta con infraestructura activa para el envío de correos electrónicos a través de servidores de Microsoft Outlook (Office 365). Esto fue verificado mediante análisis de registros MX, revelando lo siguiente:



Elemento Técnico	Resultado
Registros MX	alertiservice-com.mail.protection.outlook.com
Proveedor de correo	Microsoft Outlook 365 (AS8075)
Dirección IP asociada	52.101.68.32 (Microsoft)
Política DMARC	Publicada, pero sin política de cuarentena o rechazo (riesgo de suplantación)
Estado de SPF/DKIM/DMARC	Configurados para el dominio, pero no válidos para.gob.pe

El análisis de correo confirmaría que el dominio tiene capacidad real de envío de correos desde una plataforma legítima (Microsoft), lo que permite camuflar el phishing con mayor facilidad. La ausencia de una política DMARC restrictiva facilita la suplantación de identidad, elevando el riesgo para usuarios desprevenidos.

Este análisis confirma que el correo fue maquillado para parecer legítimo, pero en realidad es un intento de suplantación de identidad que utiliza técnicas de display name spoofing y abuso de servicios de terceros para el envío masivo.

Se ha identificado un uso indebido del nombre, imagen y símbolos de la PNP, lo que podría constituir en un delito de suplantación de identidad institucional con fines de extorsión.

No se encontraron firmas digitales oficiales ni certificados del Estado en el mensaje.

Se informó a la PNP para su revisión y acciones pertinentes.

Indicadores de Compromiso:

Campo	Detalle
Dominio	alertiservice.com
Descripción	Dominio utilizado para suplantación de identidad (PNP) mediante correos electrónicos maliciosos. Asociado a intentos de phishing y extorsión digital. detectado en campañas activas dirigidas a ciudadanos peruanos.
Registrador	RegistryGate GmbH
Fecha de creación	26 de diciembre de 2023
Fecha de expiración	26 de diciembre de 2025
Estado del dominio	clientTransferProhibited
Servidores DNS	ns5.kasserver.com, ns6.kasserver.com
IP asociada	85.13.129.145 – (Servidor Web)
IP asociada (correo)	52.101.68.32 – (Outlook 365, servicio de envío de correo)
Servidor Web	Apache – responde con HTTP/1.1 423 Locked
Infraestructura	Microsoft 365 – Outlook / Mail Protection
Ubicación IP	Alemania, Sajonia – Neue Medien Muennich GmbH
Riesgo	Alto – suplantación institucional activa
Historial de IPs	1 cambio en los últimos 2 años
Contacto de abuso:	abuse@registrygate.com

3. RECOMENDACIONES:

- Bloquear el dominio y sus IPs asociadas en sistemas institucionales.
- Hacer de conocimiento a la PNP, a través de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), sobre el incidente de suplantación de identidad institucional.
- Difundir estos IOCs entre entidades públicas, hacia los CISOs, Jefes de TI, etc.
- Monitorear registros de red, correo y DNS institucionales.
- Incluir el caso en campañas de concientización sobre suplantación digital.
- Habilitar la autenticación multifactor (MFA) en todas las plataformas que sea posible.
- No abrir enlaces ni descargar archivos sospechosos, ni responder a correos electrónicos no confiables ni mensajes de texto.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones, actualizados 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:	• Análisis propio de redes sociales, Ciberpatrullaje y Trabajo Colaborativo

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°123	Fecha: 27-05-2025 Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en la pila Bluetooth de Apache NuttX RTOS		
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:

Apache Software Foundation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo restricción incorrecta de operaciones dentro de los límites de un búfer de memoria en la pila Bluetooth del sistema operativo en tiempo real Apache NuttX RTOS (componentes HCI y UART). La explotación exitosa podría permitir que un atacante bloquee el sistema, provoque una denegación de servicio (DoS) o ejecute código arbitrario en el dispositivo afectado.

2. DETALLES:

Apache NuttX es un sistema operativo en tiempo real (RTOS) gratuito y de código abierto, diseñado para sistemas embebidos, centrado en el cumplimiento de estándares y un tamaño compacto. Es altamente escalable y compatible con una amplia gama de arquitecturas de microcontroladores, desde 8 bits hasta 64 bits, lo que lo hace ideal para todo tipo de sistemas, desde pequeños dispositivos embebidos hasta sistemas más potentes.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-35003 de tipo restricción incorrecta de operaciones dentro de los límites de un búfer de memoria en la pila Bluetooth de Apache NuttX RTOS, podría permitir a un atacante remoto no autenticado provocar una condición de DoS y la ejecución de código arbitrario.

La vulnerabilidad se debe a una restricción incorrecta de las operaciones dentro de los límites de un búfer de memoria y a condiciones de desbordamiento del búfer basadas en la pila.

Los atacantes pueden explotar potencialmente esta vulnerabilidad enviando paquetes Bluetooth especialmente diseñados maliciosamente, lo que podría provocar un fallo del sistema, DoS y la ejecución de código arbitrario. La vulnerabilidad puede explotarse de forma remota sin interacción del usuario, con vectores de ataque basados en la red.

No hay evidencia de que exista una prueba de concepto pública. Actualmente, no hay evidencia de explotación.

A. Productos afectados:

- Apache NuttX versión 7.25 hasta anteriores a 12.9.0.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Restringir y supervisar la comunicación Bluetooth.
- Implementar la segmentación de red.
- Aplicar controles de seguridad adicionales a nivel de red - Realizar un análisis de vulnerabilidades exhaustivo.

Fuente de Información:	• hxxp://www.openwall.com/lists/oss-security/2025/05/26/1 • hxxps://github.com/apache/nuttx/pull/16179 • hxxps://lists.apache.org/thread/k4xzz3jhkx48zxw9vwmqrmm4hmg78vsj

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°123	Fecha: 27-05-2025 Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en la herramienta de configuración iSTAR (ICU) de Johnson Controls		
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:

Johnson Controls Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo uso de variables no inicializadas que afecta a la herramienta de utilidad de configuración iSTAR (ICU), ampliamente utilizada en sectores de infraestructura crítica como instalaciones comerciales, manufactura, energía, gobierno y sistemas de transporte. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener acceso a la memoria filtrada de la UCI.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-26383 de tipo uso de variables no inicializadas que afecta a la herramienta de utilidad de configuración iSTAR (ICU), podría permitir a un atacante remoto no autenticado obtener acceso a la memoria filtrada de la UCI, lo que podría resultar en la exposición involuntaria de datos confidenciales o no autorizados.

La vulnerabilidad no requiere autenticación ni interacción del usuario y puede explotarse a través de la red donde se accede a la herramienta ICU. La herramienta iSTAR ICU pierde memoria, lo que podría generar una exposición no deseada de datos no autorizados.

A. Productos afectados:

- iSTAR Configuration Utility (ICU): todas las versiones anteriores a la 6.9.5.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Restringir el acceso de red a la herramienta ICU únicamente a usuarios y redes confiables.
- Revisar periódicamente los registros y monitoree si hay señales de explotación o acceso no autorizado a los datos.

Fuente de Información:	• hxxps://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories • hxxps://us-cert.cisa.gov/news-events/ics-advisories/icsa-25-146-01 • hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-146-01

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°123	Fecha: 27-05-2025 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en el kit de herramientas NVIDIA CUDA		
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 publicado una vulnerabilidad de severidad **ALTA** de tipo corrupción de memoria que afecta al Kit de herramientas CUDA de NVIDIA en todas las plataformas. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

NVIDIA CUDA Toolkit es un entorno de desarrollo integral diseñado para crear aplicaciones de alto rendimiento aceleradas por GPU. Permite a los desarrolladores crear, optimizar e implementar aplicaciones en una amplia gama de plataformas, como sistemas integrados, estaciones de trabajo de escritorio, centros de datos empresariales, plataformas en la nube y supercomputadoras.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-23247 de tipo corrupción de memoria que afecta al Kit de herramientas CUDA de NVIDIA, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad existe debido a un error de límite en el binario uobjdump. Un atacante remoto puede crear un binario ELF especialmente diseñado, engañar a la víctima para que lo pase a la aplicación, provocar corrupción de memoria y ejecutar código arbitrario en el sistema objetivo. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

No existen informes detallados actuales sobre campañas de explotación activa generalizadas o sostenidas. Por lo tanto, si bien la vulnerabilidad es explotable y representa un riesgo, el nivel de explotación activa por parte de los actores de amenazas parece limitado o no ampliamente reportado en este momento.

A. Productos afectados:

- NVIDIA CUDA Toolkit: 12.8.1 (todas las plataformas).

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://nvidia.custhelp.com/app/answers/detail/a_id/5643

Índice alfabético

Explotación de vulnerabilidades conocidas 7, 8, 9
Suplantación 4