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

097-2025-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°097	Fecha: 25-04-2025
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Ciberdelincuentes aprovechan la muerte del papa Francisco para lanzar estafas		
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:

Cada vez que ocurre una noticia importante, observamos un aumento drástico de las estafas diseñadas para explotar el interés público.

En medio del impacto global generado por la muerte del papa Francisco, Check Point Research detectó una amenaza con una oleada de ciberataques diseñados por grupos delictivos que buscan aprovecharse del interés masivo y la conmoción colectiva para ejecutar estafas digitales, robar datos sensibles y propagar desinformación.

2. DETALLES:

El método más común comienza con publicaciones virales en redes sociales como Instagram, TikTok o Facebook, donde se difunden imágenes generadas por inteligencia artificial, para simular mensajes póstumos del papa, supuestos comunicados del Vaticano o incluso peticiones de ayuda urgentes.

Estas piezas falsas, diseñadas para captar la atención, redirigen a los usuarios hacia sitios fraudulentos que solicitan donaciones urgentes, datos bancarios para acceder a las cuentas y robar todo lo que puedan, o simplemente buscan robar credenciales mediante formularios camuflados para suplantar la identidad y realizar diferentes actividades con nuestra información.

En uno de los casos detectados, al hacer clic en un enlace camuflado, el internauta era llevado a una página falsa de Google que promovía supuestas tarjetas de regalo que, en realidad, eran una estafa.

Algunas de estas webs falsas ejecutan comandos en segundo plano sin que el usuario lo note.

Este tipo de ataque recopila datos técnicos del dispositivo, como el nombre del equipo, sistema operativo, país o idioma, con el objetivo de lanzar ataques dirigidos o vender la información en la Dark Web.

Una amenaza creciente es el “envenenamiento SEO”, una estrategia en la que los atacantes posicionan sus páginas entre los primeros resultados de búsqueda para eventos relevantes. Por ejemplo, una persona que buscaba noticias sobre el Papa podía terminar en un sitio malicioso que aparentaba ser legítimo. Estos dominios suelen ser nuevos o previamente inactivos, lo que les permite evadir los filtros de seguridad tradicionales.

3. RECOMENDACIONES:

- No abrir archivos adjuntos ni enlaces presentes en correos electrónicos sospechosos ni en otros mensajes, ni descargar desde sitios que no sean oficiales.
- También se debe mantener el sistema operativo, software antimalware y de seguridad, y todas las aplicaciones, actualizadas con los últimos parches y actualizaciones de seguridad.
- Usar extensiones de verificación de sitios web.
- Denunciar el contenido fraudulento para ayudar a frenar su propagación.

Fuente de Información:	• hxxps://sinmordaza.com/noticia/450850-ciberdelincuentes-aprovechan-la-muerte-del-papa-francisco-para-lanzar-estafas.html • hxxps://www.elindependiente.com/sociedad/2025/04/25/estafas-bulos-papa-francisco/ • hxxps://www.infobae.com/tecno/2025/04/25/encuentran-noticias-falsas-sobre-la-muerte-del-papa-francisco-que-roba-dinero-de-los-feligreses/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°097	Fecha: 25-04-2025 Página: 5 de 8

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

Se ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo desbordamiento de búfer basado en pila que afecta a la herramienta de configuración iSTAR (ICU) de Johnson Controls, Inc. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-26382 de tipo desbordamiento de búfer basado en pila que afecta a la herramienta de configuración iSTAR (ICU), podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en los sistemas afectados, lo que podría comprometer por completo la confidencialidad, la integridad y la disponibilidad.

La vulnerabilidad es explotable de forma remota, con baja complejidad de ataque y no requiere autenticación o interacción del usuario.

A. Productos afectados:

- UCI: Versiones anteriores a la versión 6.9.5.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Minimizar la exposición de la red para los dispositivos del sistema de control (no deben ser accesibles desde Internet).
- Colocar las redes del sistema de control y los dispositivos remotos detrás de cortafuegos y aislarlos de las redes comerciales.
- Utilizar métodos seguros como VPN para el acceso remoto, las VPN deben estar actualizadas.
- Monitorear la actividad sospechosa de la red y aislar los sistemas afectados si no es posible aplicar parches inmediatamente.

Fuente de Información:	• hxxps://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories • hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-114-05

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°097	Fecha: 25-04-2025 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades de severidad crítica en SAP NetWeaver		
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 dos vulnerabilidades de severidad **CRÍTICA** de tipo deserialización de datos no confiables y carga de archivos arbitrarios en SAP NetWeaver. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y comprometer el sistema vulnerable.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2017-9844 de tipo deserialización de datos no confiables en SAP NetWeaver, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada insegura al procesar datos serializados en el Cargador de Metadatos del servidor de desarrollo de Visual Composer. Un atacante remoto no autenticado puede pasar datos especialmente diseñados a la aplicación y ejecutar código arbitrario en el sistema objetivo. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-31324 de tipo carga de archivos arbitrarios en SAP NetWeaver, podría permitir que un atacante remoto comprometa el sistema vulnerable. La vulnerabilidad existe debido a una validación insuficiente del archivo durante la carga en el Cargador de Metadatos del servidor de desarrollo de Visual Composer. Un atacante remoto no autenticado puede cargar un archivo malicioso y ejecutarlo en el servidor. Esta vulnerabilidad está siendo explotado activamente en la naturaleza.

A. Productos afectados:

- SAP NetWeaver: 7.4.
- SAP NetWeaver: 7,50.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://me.sap.com/notes/2399804 • hxxps://me.sap.com/notes/3594142 • hxxps://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html • hxxps://reliaquest.com/blog/threat-spotlight-reliaquest-uncovers-vulnerability-behind-sap-netweaver-compromise/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°097	Fecha: 25-04-2025
		Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de escalada de privilegios locales en Avast Free Antivirus		
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:

Avast Software ha publicado una vulnerabilidad de severidad **ALTA** de tipo desbordamiento de enteros en Avast Free Antivirus. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante local escalar privilegios en las instalaciones afectadas de Avast Free Antivirus.

2. DETALLES:

Avast Free Antivirus, es una versión gratuita para uso doméstico con protección básica contra virus y malware, que incluye funciones como escaneo HTTPS, antiphishing y protección contra ransomware.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-3500 de tipo desbordamiento de enteros en Avast Free Antivirus, podría permitir a un atacante local escalar privilegios en las instalaciones afectadas de Avast Free Antivirus. Para explotar esta vulnerabilidad, un atacante debe primero ejecutar código con pocos privilegios en el sistema objetivo.

La falla específica existe en el controlador del kernel aswbidsdriver. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar un desbordamiento de enteros antes de asignar un búfer. Un atacante puede aprovechar esta vulnerabilidad para escalar privilegios y ejecutar código arbitrario en el contexto del kernel.

A. Productos afectados:

- Avast Free Antivirus, múltiples versiones.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.zerodayinitiative.com/advisories/ZDI-25-256/

Índice alfabético