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

107-2025-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°107	Fecha: 08-05-2025
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Hallan un nuevo y peligroso kit de smishing llamado Panda Shop		
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:

La firma de seguridad estadounidense Resecurity ha identificado la existencia de un nuevo kit de smishing conocido como 'Panda Shop' que imita las tácticas de Smishing Triad con características mejoradas y nuevas plantillas.

2. DETALLES:

Se sirve de un modelo Crime-as-a-Service (delito-como-servicio) de tal manera que cualquiera puede disponer de esta arma por un módico precio. Así, fácilmente pueden escalar sus operaciones dirigidas a consumidores en distintos países.

El kit de smishing se puede adquirir a través del servicio de atención al cliente o mediante un bot automatizado de Telegram. Los creadores del kit también ofrecen manuales interactivos sobre su uso.

Los investigadores han señalado que los principales métodos usados son a través de Google RCS, Apple iMessage, y pasarelas de SMS para entrega del smishing, A ellos también se les suman los foros o redes sociales, como Facebook, X (Twitter) o Reddit.

Panda Shop contaría con múltiples canales de Telegram y bots interactivos para automatizar la prestación de servicios. Los ciberdelincuentes chinos se sienten más cómodos usando Telegram, que plataformas de mensajería instantánea chinas, cuando se trata de participar en actividades ilegales.

Los remitentes a menudo se hacen pasar por entidades que sus víctimas “conocen” de alguna manera: instituciones financieras, minoristas, superiores laborales y agencias de servicio civil son ejemplos comunes. De ahí logran ganarse la confianza de la víctima para luego explotarla, defraudarla y robarle información privada o dinero.

El espectro de delitos cometidos mediante smishing abarca desde el fraude tradicional con tarjetas y NFC hasta las cadenas de blanqueo de capitales, que permiten a los estafadores procesar fondos robados.

3. RECOMENDACIONES:

- Estar alerta a los ataques de ingeniería social.
- Buscar señales un posible phishing.
- Verificar primero la autenticidad del origen.
- Actualizar las credenciales que pudieran estar comprometidas.
- Implementar una arquitectura integral de cero confianza para minimizar la superficie de ataque, prevenir el compromiso, eliminar el movimiento lateral y detener la pérdida de datos.

Fuente de Información:	• hxxps://www.escudodigital.com/ciberseguridad/hallan-nuevo-peligroso-kit-smishing-llamado-panda-shop_63261_102.html • hxxps://www.resecurity.com/blog/article/smishing-massive-scale-panda-shop-chinese-carding-syndicate • hxxps://securityaffairs.com/177502/cyber-crime/smishing-on-a-massive-scale-panda-shop-chinese-carding-syndicate.html • hxxps://www.scworld.com/brief/colossal-chinese-panda-shop-smishing-campaign-examined

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°107	Fecha: 08-05-2025
		Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en complemento Django		
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:

Django Software Foundation ha publicado una vulnerabilidad de severidad **MEDIA** de tipo denegación de servicio (DoS), que afecta específicamente a la función django.utils.html.strip_tags() función. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto realizar un ataque de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-32873 de tipo denegación de servicio (DoS), podría permitir a un atacante remoto realizar un ataque de denegación de servicio (DoS) explotando el procesamiento lento en la strip_tags()función. Esta función puede ser lenta al evaluar ciertas entradas, lo que podría explotarse para causar una condición de denegación de servicio.

A. Productos afectados:

- Django 5.0.
- Django 5.2.
- Django 4.0.
- Django 4.2.20.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//docs[.]djangoproject[.]com/es/dev/releases/security/ • hxxps[:]//groups.google[.]com/g/django-announce • hxxps[:]//www[.]djangoproject[.]com/weblog/2025/may/07/releases-de-seguridad/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°107	Fecha: 08-05-2025 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en productos de Danfoss		
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:

Danfoss ha publicado una vulnerabilidad de severidad **ALTA** de tipo autenticación incorrecta, que afecta a la serie Danfoss AK-SM 8xxA anterior a la versión 4.2. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante eludir los controles normales de acceso y obtener acceso sin credenciales válidas.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-41450 de tipo autenticación incorrecta, podría permitir a un atacante eludir los controles normales de acceso y obtener acceso sin credenciales válidas. Permite el acceso no autorizado a sistemas afectados debido a una debilidad en el mecanismo de autenticación.

A. Productos afectados:

- Danfoss AK-SM 8xxA anteriores a 4.2.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//sm800a[.]danfoss[.]com/sw_shared/SM800A-4.2.4.spk

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°107	Fecha: 08-05-2025 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad se severidad crítica en complemento de Wordfence		
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:

WordPress Org. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo escalada de privilegios, que afecta al plugin Job Listings para WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto eludir las comprobaciones de autorización.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-3918 de tipo escalada de privilegios, podría permitir a un atacante remoto eludir las comprobaciones de autorización.

El problema surge de una autorización incorrecta en la register_action() función del plugin, que utiliza directamente la información proporcionada por el cliente $_POST['user_role'] al crear cuentas de usuario sin restringirla a un conjunto seguro de roles. Esta falla permite a un atacante no autenticado escalar privilegios al nivel de administrador, lo que wp_insert_user () podría permitirle obtener el control total del sitio de WordPress afectado.

A. Productos afectados:

- Plugin Job Listings para WordPress, versiones 0.1 a 0.1.1.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//www[.]Wordfence[.]com/threat-intel/vulnerabilities/wordpress-plugins/job-listings/job-listings-01-011-unauthenticated-privilege-escalation-via-register-action-function • hxxps[:]//plugins[.]trac.wordpress[.]org/browser/job-listings/trunk/includes/forms/class-jlt-form-member.php#L68 • hxxps[:]//wordpress[.]org/plugins/job-listings/#developers

Índice alfabético