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

117-2025-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

Fraude por medio de mensajes de texto son cada vez más recurrentes 4
Vulnerabilidad de severidad crítica en el router Netgear DGND3700 5
Vulnerabilidad de severidad crítica en el router TP-Link Archer AX50 6
Múltiples vulnerabilidades en VMware Cloud Foundation 7
Vulnerabilidad crítica en el servidor de panel inalámbrico PrismaSeT Active de Schneider Electric 8
Índice alfabético 9

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°117	Fecha: 20-05-2025
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Fraude por medio de mensajes de texto son cada vez más recurrentes		
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:

Una de las amenazas digitales más notorias en los últimos años ha sido la proliferación de ataques de phishing conocida como smishing, que consiste en falsos mensajes de texto, que suplantan la identidad de alguna entidad.

2. DETALLES:

El smishing es una técnica de ingeniería social que utiliza un pretexto para influir en sus víctimas y obligarlas a actuar, a través del SMS. La noción de pretexto es un elemento crucial de cualquier intento de ingeniería social. Por ejemplo, en un ataque dirigido a los empleados de una empresa, el atacante podría usar una actualización de VPN como pretexto para lograr que ingresen sus credenciales en una página de autenticación falsa bajo su control.

Ya sea que el atacante distribuya malware a través de una plataforma en línea o robe credenciales de inicio de sesión, generalmente incluirá al menos un enlace a un dominio bajo su control en el cuerpo del SMS.

Estos ataques utilizan una combinación de manipulación tecnológica y tácticas psicológicas para engañar a las víctimas para que faciliten información personal, bancaria o incluso realicen pagos sin percatarse de que están siendo víctima de un fraude.

Todo comienza con un SMS que aparenta ser una notificación oficial, contiene un enlace que lo redirige a una copia casi perfecta del portal real. Los logotipos, tipografías y estructura visual han sido replicados con precisión, incluso en algunos casos, han sido diseñados con herramientas de Inteligencia Artificial. El usuario, confiado, introduce sus datos de contacto, tarjeta de crédito o incluso su número de cuenta. A partir de ese momento, los ciberdelincuentes obtienen el acceso necesario para realizar cargos, vaciar cuentas o vender los datos en el mercado negro digital.

El éxito de este tipo de fraude radica en la habilidad de los atacantes para suplantar entidades conocidas y generar una sensación de urgencia. Aprovechan momentos de alta actividad comercial, como Navidad o el Black Friday, cuando los usuarios están esperando varios envíos y es más probable que no duden ante un aviso de entrega.

Hay diferentes temáticas para este tipo de ataque como las estafas de verificación de cuenta, de premios o loterías, de soporte técnico, alertas de fraude bancario, cancelación de servicios, y ofertas para devoluciones de impuestos o descargar aplicaciones deseadas.

Existen varias señales que pueden alertarnos como enlaces acortados, errores ortográficos o sintaxis extraña, y mensajes que piden datos confidenciales o pagos inmediatos.

3. RECOMENDACIONES:

- Tener cuidado con los enlaces en los mensajes de texto, incluso si parecen dirigir a sitios web reales.
- Verificar siempre antes de introducir la información de inicio de sesión.
- 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:	
	• hxxps://www.escudodigital.com/ciberseguridad/caso-falsos-sms-correos-operan-ciberdelincuentes_63418_102.html • hxxps://www.proofpoint.com/es/threat-reference/smishing

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°117	Fecha: 20-05-2025
		Página: 5 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el router Netgear DGND3700		
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 autenticación incorrecta que afecta al router Netgear DGND3700. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir los controles de autenticación y obtener acceso no autorizado al dispositivo.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-4978 de tipo autenticación incorrecta que afecta al router Netgear DGND3700. El problema reside en el mecanismo de autenticación básica del dispositivo, en particular en el /BRS_top.htmlcomponente, podría permitir a un atacante remoto no autenticado eludir los controles de autenticación y potencialmente obtener acceso no autorizado al dispositivo. La explotación exitosa puede llevar al compromiso total del dispositivo, incluidos impactos en la confidencialidad, integridad y disponibilidad.

El exploit se ha hecho público y está disponible para su uso por parte de atacantes.

A. Productos afectados:

- Router Netgear DGND3700, versión de firmware 1.1.00.15_1.00.15NA.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de firmware disponible que aborda esta vulnerabilidad.
- Restringir el acceso remoto al dispositivo hasta que haya una solución disponible.
- Monitorear actividad inusual en los dispositivos afectados.

Fuente de Información:	• hxxps://github.com/at0de/my_vulns/blob/main/Netgear/DGND3700v2/backdoor.md • hxxps://github.com/at0de/my_vulns/blob/main/Netgear/DGND3700v2/backdoor.md • hxxps://vuldb.com/?ctiid.309639 • hxxps://vuldb.com/?id.309639 • hxxps://vuldb.com/?submit.564712 • hxxps://www.netgear.com/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°117	Fecha: 20-05-2025 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el router TP-Link Archer AX50		
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 al binario "conn-indicator" que se ejecuta como root en el router TP-Link Archer AX50. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario con privilegios de root en el enrutador, lo que podría provocar un compromiso total del dispositivo.

2. DETALLES:

La vulnerabilidad de severidad crítica identificada por MITRE como CVE-2025-40634 de tipo desbordamiento de búfer basado en pila que afecta al binario "conn-indicator" que se ejecuta como root en el router TP-Link Archer AX50, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y obtener el control total del enrutador afectado.

Un atacante podría ejecutar código arbitrario en el dispositivo a través de redes LAN y WAN. La vulnerabilidad crítica tiene un gran impacto en la confidencialidad, la integridad y la disponibilidad.

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

A. Productos afectados:

- Router TP-Link Archer AX50, versiones de firmware anteriores a la 1.0.15 compilación 241203 rel61480.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Restringir el acceso de red al enrutador desde redes no confiables.
- Implementar la segmentación de red.
- Monitorear cualquier actividad de red sospechosa.
- Considerar aislar temporalmente el dispositivo de las redes no confiables, en caso que la actualización no haya sido posible de inmediato.

Fuente de Información:	• hxxps://www.incibe.es/en/incibe-cert/notices/aviso/stack-based-buffer-overflow-tp-link-archer-ax50

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°117	Fecha: 20-05-2025 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en VMware Cloud Foundation		
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:

Broadcom Inc. ha publicado múltiples vulnerabilidades de severidad **ALTA** de tipo recorrido de ruta, exposición de información sensible a un actor no autorizado y autorización faltante que afectan a VMware Cloud Foundation (VCF). La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto obtener acceso no autorizado a servicios internos y acceder a información confidencial.

2. DETALLES:

VMware Cloud Foundation es una plataforma integral de centro de datos definido por software (SDDC), diseñada para simplificar la implementación y la gestión de la infraestructura de nube privada.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-41229 de tipo recorrido de ruta, podría permitir a un agente malicioso con acceso de red al puerto 443 de VMware Cloud Foundation explotar este problema para acceder a ciertos servicios internos. Esta vulnerabilidad no requiere privilegios ni interacción del usuario para explotarse.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-41230 de tipo exposición de información sensible a un actor no autorizado, podría permitir a un agente malicioso con acceso al puerto 443 de VMware Cloud Foundation explotar este problema para acceder a información confidencial.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-41231 de tipo autorización faltante, podría permitir a un agente malicioso con acceso al dispositivo VMware Cloud Foundation podría realizar ciertas acciones no autorizadas y acceder a información confidencial limitada.

Estas vulnerabilidades suponen un riesgo significativo para los entornos empresariales, ya que podrían exponer servicios internos e información confidencial a atacantes no autorizados. Las organizaciones que utilizan VMware Cloud Foundation deben priorizar la aplicación de las actualizaciones de seguridad y considerar la segmentación de la red para reducir la exposición hasta que se apliquen los parches.

A. Productos afectados:

- VMware Cloud Foundation, versiones 4.5.x de Cloud Foundation sin el parche de seguridad KB398008.
- VMware Cloud Foundation, versiones 5.x de Cloud Foundation anteriores a la 5.2.1.2.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25733

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°117	Fecha: 20-05-2025 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en el servidor de panel inalámbrico PrismaSeT Active de 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 ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo desbordamiento de búfer clásico que afecta al servidor de panel inalámbrico PrismaSeT Active. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución de código no autorizado, lo que podría resultar en la falta de disponibilidad del PrismaSeT Active - Wireless Panel Server para el monitoreo de pérdida de voltaje.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2023-4041 de tipo desbordamiento de búfer clásico que afecta al servidor de panel inalámbrico PrismaSeT Active de Schneider Electric, podría permitir a un atacante remoto no autenticado la ejecución de código no autorizado, lo que podría resultar en la falta de disponibilidad del PrismaSeT Active - Wireless Panel Server para el monitoreo de pérdida de voltaje.

La vulnerabilidad de desbordamiento de búfer clásico, escritura fuera de límites, descarga de código sin verificación de integridad en el cargador de arranque Gecko de Silicon Labs en ARM (módulos del analizador de archivos de actualización de firmware) permite la inyección de código y la omisión de la autenticación. Este problema afecta a las versiones "Independiente" y "Aplicación" del cargador de arranque Gecko.

A. Productos afectados:

- PrismaSeT Active - Servidor de panel inalámbrico: Todas las versiones.

3. RECOMENDACIONES:

- Cambiar de dispositivo o asumir el riesgo, ya que el producto PrismaSeT Active - Wireless Panel Server ha llegado al final de su vida útil y ya no recibe soporte.
- Para reducir el riesgo de explotación se debe desactivar la comunicación Bluetooth Low (BLE) del servidor de panel inalámbrico cuando no esté en uso.
- Revisar periódicamente los registros de auditoría y/o las notificaciones de seguridad de la aplicación EcoStruxure Facility Expert para detectar comportamientos inesperados.
- Verificar periódicamente la seguridad física del servidor de panel inalámbrico para protegerlo contra el emparejamiento Bluetooth no autorizado.
- Utilizar únicamente la aplicación oficial EcoStruxure Power Commission y la aplicación EcoStruxure Facility Expert de Schneider Electric, disponibles en Google Play Store y Apple App Store.
- No utilizar la aplicación EcoStruxure Power Commission ni la aplicación EcoStruxure Facility Expert en dispositivos móviles rooteados o con jailbreak.
- Seguir las recomendaciones de ciberseguridad del servidor de panel inalámbrico PrismaSeT Active.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-140-06 • hxxps://www.se.com/en/work/support/cybersecurity/security-notifications.jsp • hxxps://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-133-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-133-04.pdf

Índice alfabético

Explotación de vulnerabilidades conocidas 5, 6, 7, 8
Suplantación 4