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

136-2025-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°136	Fecha: 12-06-2025
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Nueva estafa en Instagram busca robar cuentas haciéndose pasar por el soporte técnico de Meta		
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:**

En Instagram ha surgido una nueva estafa, que está enfocada en afectar a influencers, pequeñas empresas y creadores de contenido que dependen de esta plataforma para mantener su presencia en línea y, en muchos casos, sus ingresos.

2. **DETALLES:**

Los estafadores, pretendiendo ser el soporte técnico de Meta, inician el contacto mediante mensajes directos enviados a los perfiles de los objetivos.

El mensaje, que informa falsamente sobre la violación de políticas de Meta, advierte que la cuenta del usuario será desactivada si no se toma acción inmediata.

Se incluye un enlace en el mensaje, que lleva a la víctima a una página que imita fielmente al Centro de Soporte de Publicidad de Meta.

Ahí es donde se les pide a los usuarios que inicien un proceso de "verificación de cuenta", proporcionando su nombre de usuario de Instagram, contraseña, y, en muchos casos, el código para la autenticación de dos factores.

Este acceso no autorizado permite a los estafadores controlar la cuenta en cuestión, expulsando al propietario legítimo y explotando a los seguidores de la cuenta secuestrada.

Los datos recopilados se venden en mercados clandestinos de la Deep Web, o se exige un rescate económico a los propietarios de las cuentas para devolverles el acceso.

Los ataques como éste pueden facilitar otros crímenes cibernéticos, incluidos el robo de identidad y el uso no autorizado de información personal, como son:

- **Pérdida Financiera:** Los usuarios pueden perder acceso a sus cuentas monetizadas o aquellas vinculadas a servicios financieros.
- **Robo de Identidad:** La exposición de información personal puede ser utilizada para realizar fraudes adicionales.
- **Aumento en la Cibercriminalidad:** El éxito de estos esquemas puede alentar a otros delincuentes a adoptar tácticas similares.

Además, contribuyen a una erosión generalizada de la confianza en plataformas digitales y servicios online

3. **RECOMENDACIONES:**

- Nunca compartir contraseñas o datos personales con terceros no verificados.
- Dirigirse directamente al sitio web oficial para verificar cualquier notificación antes de actuar, en caso reciba algún mensaje sobre problemas con su cuenta.
- Activar la autenticación en dos pasos puede agregar una capa adicional de seguridad a tu cuenta.
- Evita hacer clic en enlaces enviados por desconocidos; verifica siempre su procedencia antes de ingresar información personal.

Fuente de Información:	• hxxps://enigmasecurity.cl/noticias-2187/ • hxxps://www.infobae.com/tecno/2025/06/12/nueva-estafa-en-instagram-busca-robar-cuentas-haciendose-pasar-por-el-soporte-tecnico-de-meta/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°136	Fecha: 12-06-2025 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Energy Services de Siemens		
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:

Siemens AG ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo permisos predeterminados incorrectos que afecta a todas las versiones de Siemens Energy Services que utilizan el componente G5DFR. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener control remoto del componente G5DFR y manipular las salidas del dispositivo, comprometer la integridad del sistema, manipular o modificar las operaciones del dispositivo y acceder al sistema sin autenticación.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-40585 de tipo permisos predeterminados incorrectos que afecta a Energy Services, podría permitir a un atacante remoto no autenticado obtener control remoto del componente G5DFR y manipular las salidas del dispositivo. La vulnerabilidad no es compleja debido al uso de credenciales predeterminadas y no requiere autenticación o interacción del usuario.

Las soluciones afectadas que utilizan G5DFR contienen credenciales predeterminadas. Esto podría permitir que un atacante tome el control del componente G5DFR y altere las salidas del dispositivo.

A. Productos afectados:

- Siemens Energy Services: todas las versiones con G5DFR.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Utilizar la interfaz web de G5DFR para cambiar los nombres de usuario, las contraseñas y los niveles de permiso predeterminados.
- Implementar mecanismos de autenticación únicos y fuertes.
- Restringir el acceso de red al componente G5DFR.
- Realizar auditorías de seguridad integrales.
- Monitorizar intentos de acceso no autorizado.
- Considerar la segmentación de la red para aislar los componentes vulnerables.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-162-06 • hxxps://cert-portal.siemens.com/productcert/html/ssa-345750.html • hxxps://www.siemens.com/cert/operational-guidelines-industrial-security

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°136	Fecha: 12-06-2025 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades de severidad crítica en Endpoint Encryption PolicyServer de Trend Micro		
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:

Trend Micro ha publicado dos vulnerabilidades de severidad **CRÍTICA** de tipo deserialización de datos no confiables que afecta a Trend Micro Endpoint Encryption, específicamente al componente PolicyServer. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código arbitrario como SYSTEM en el servidor afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-49212 de tipo deserialización de datos no confiables en Endpoint Encryption PolicyServer, 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 la clase *PolicyValueTableSerializationBinder*, debido a una validación insuficiente de la entrada proporcionada por el usuario. 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-2025-49213 de tipo deserialización de datos no confiables que afecta a Trend Micro Endpoint Encryption PolicyServer, específicamente a la clase *PolicyServerWindowsService*, podría permitir a un atacante remoto ejecutar código arbitrario en los sistemas afectados sin necesidad de autenticación, lo que podría permitirle obtener privilegios de nivel SYSTEM. La vulnerabilidad existe debido a una validación de entrada insegura al procesar datos serializados. Un atacante remoto 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.

A. Productos afectados:

- Trend Micro Endpoint Encryption PolicyServer: anterior a la versión 6.0.0.4013.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión 6.0.0.4013 que aborda esta vulnerabilidad. Trend Micro ha publicado actualizaciones de seguridad para abordar estas vulnerabilidades. Las organizaciones que utilizan Endpoint Encryption PolicyServer deben aplicar los parches más recientes de inmediato para mitigar el riesgo.

Fuente de Información:	• hxxps://success.trendmicro.com/en-US/solution/KA-0019928 • hxxps://www.zerodayinitiative.com/advisories/ZDI-25-369/ • hxxps://www.zerodayinitiative.com/advisories/ZDI-25-370/ • hxxps://www.zerodayinitiative.com/advisories/ZDI-25-371/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°136	Fecha: 12-06-2025
		Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en la función SD-WAN del software PAN-OS® de Palo Alto Networks		
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 **MEDIA** de tipo exposición de información sensible del sistema a una esfera de control no autorizada que afecta a la función SD-WAN del software PAN-OS® de Palo Alto Networks. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado acceder a datos no cifrados enviados desde el firewall a través de la interfaz SD-WAN. Esto requiere que el usuario pueda interceptar los paquetes enviados desde el firewall.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-4229 de tipo exposición de información sensible del sistema a una esfera de control no autorizada que afecta a Palo Alto PAN-OS, podría permitir a un atacante remoto comprometa el sistema objetivo. La vulnerabilidad existe debido a la exposición de información confidencial del sistema a una esfera de control no autorizada en la función SD-WAN. Un atacante remoto puede acceder a dicha información confidencial.

Para ser vulnerable a este problema, se debe configurar un perfil de interfaz SD-WAN en PAN-OS. La interfaz también debe estar configurada para acceso directo a Internet (DIA). Para agregar un perfil de interfaz SD-WAN se requiere la licencia SD-WAN avanzada.

A. Productos afectados:

- Palo Alto PAN-OS: 10.1.0, 10.1.1, 10.1.2, 10.1.3, 10.1.4, 10.1.5, 10.1.6, 10.1.7, 10.1.8, 10.1.9, 10.1.10, 10.1.11, 10.1.12, 10.1.13, 10.1.14, 10.1.14-h1, 10.1.14-h2, 10.1.14-h3, 10.1.14-h4, 10.1.14-h5, 10.1.14-h6, 10.1.14-h7, 10.1.14-h8, 10.1.14-h9, 10.1.14-h10, 10.1.14-h11, 10.1.14-h13, 10.1.14-h14, 10.1.14-h15, 10.2.0, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.2.8, 10.2.9, 10.2.10, 10.2.11, 10.2.12, 10.2.13, 10.2.14, 10.2.15, 10.2.16, 11.1.0, 11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.1.5, 11.1.6, 11.1.8, 11.1.9, 11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.2.6.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad. Si no utiliza la función SD-WAN de PAN-OS, puede solucionar este problema desactivándola.

Fuente de Información:	• hxxps://security.paloaltonetworks.com/CVE-2025-4229

Índice alfabético