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

105-2025-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°105	Fecha: 06-05-2025
		Página: 4 de 11

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Hackean versión modificada de Signal usada por el Gobierno de EEUU		
Tipo de Ataque	Fuga de Información	Abreviatura	FugaInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K02
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. **ANTECEDENTES:**

La Administración de Donald Trump se enfrenta a una nueva brecha de seguridad porque un hacker ha explotado una vulnerabilidad en TeleMessage para acceder a los mensajes archivados y otros datos relacionados con los funcionarios del Gobierno estadounidense.

TeleMessage proporciona versiones modificadas de apps de mensajería cifradas como Signal, Telegram, WhatsApp y WeChat; esta aplicación es utilizada por parte del gobierno estadounidense para archivar mensajes, ya que entre sus posibilidades ofrece la opción de archivar texto y audios de forma segura.

Funcionarios del Gobierno estadounidense utilizan esta aplicación, incluido el exasesor de Seguridad Nacional de la Casa Blanca, Mike Waltz, quien desveló recientemente y de manera accidental el uso de este servicio en una reunión de gabinete.

2. **DETALLES:**

Tras dar a conocer que algunos funcionarios de alto rango del Gobierno de Estados Unidos utilizan esta aplicación, el hacker aprovechó una serie de vulnerabilidades presentes en la modificación de Signal, que permitieron al ciberatacante acceder a los registros de las conversaciones archivadas, ya que no estaban protegidas con encriptación de extremo a extremo

Según indica el medio 404Media, el hacker no ha accedido a los mensajes ni a la información de contacto de los usuarios ni a sus credenciales de acceso. Aunque sí pudo obtener datos de la Oficina de Aduanas y Protección Fronteriza, la plataforma de intercambio de criptomonedas Coinbase y proveedores de servicios financieros como Scotiabank, según se aprecia en las capturas de pantalla de mensajes y sistemas 'backend' obtenidos por el medio.

Por su lado, Signal, a quien este escándalo también le ha salpicado al tratarse de una versión modificada de su aplicación, ha explicado que "no podemos garantizar la privacidad ni la seguridad de las versiones no oficiales de Signal". En la práctica, son dos aplicaciones diferentes. Signal es un proyecto de código abierto que puede ser utilizado por otros desarrolladores para lanzar sus propios proyectos y aplicaciones. Precisamente una de las aplicaciones que han nacido a raíz de Signal es TeleMessage, pero no existe vinculación entre ambas.

Por otro lado, el Departamento de Seguridad Nacional de Estados Unidos afirma que los funcionarios de aduanas han desactivado la aplicación en sus dispositivos por precaución.

3. **RECOMENDACIONES:**

- No instalar ni descargar instaladores de aplicaciones desde sitios que no sean oficiales.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas 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.20minutos.es/tecnologia/ciberseguridad/trump-sufre-brecha-seguridad-version-signal-usada-altos-funcionarios-ha-sido-hackeada-5706701/ • hxxps://www.infobae.com/america/agencias/2025/05/05/hackean-una-version-modificada-de-signal-que-utiliza-el-gobierno-de-estados-unidos/ • hxxps://www.xatakamovil.com/seguridad/telemessage-prueba-que-nada-sirve-usar-apps-seguras-como-signal-no-sabes-como-se-utilizan

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°105	Fecha: 06-05-2025 Página: 5 de 11

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

SonicWall Inc. ha publicado una vulnerabilidad de severidad **MEDIA** de tipo resolución incorrecta de enlaces que afecta a clientes de Windows SonicWall Connect Tunnel. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario local realizar un ataque de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-32817 de tipo resolución incorrecta de enlaces, podría permitir a un usuario local realizar un ataque de DoS.

Esta falla permite a un atacante local con privilegios reducidos explotar la forma en que el cliente resuelve nombres de archivos que pueden ser enlaces simbólicos o accesos directos, lo que provoca sobrescrituras no autorizadas de archivos.

A. Productos afectados:

- SonicWall Connect Tunnel, versión 12.4.3.283 y anteriores de las plataformas de Windows 64 bit y 32 bit.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión 12.4.3.298 o posterior. No existen soluciones alternativas conocidas.

Fuente de Información:	• hxxps[:]//psirt[.]global[.]sonicwall[.]com/vuln-detail/SNWLID-2025-0007

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°105	Fecha: 06-05-2025 Página: 5 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en productos D-Link		
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:

D-Link Corporation ha publicado una vulnerabilidad de severidad **MEDIA** de tipo inyección de comandos que afecta específicamente a versiones de firmware hasta la 104WWb01. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar comandos arbitrarios en el dispositivo vulnerable.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-4341 de tipo inyección de comandos, podría permitir a un atacante manipular ciertos argumentos del encabezado HTTP (HTTP_ST, REMOTE_ADDR, REMOTE_PORT, SERVER_ID) para ejecutar comandos arbitrarios en el dispositivo de forma remota.

Esta vulnerabilidad afecta únicamente a los modelos que ya no son compatibles con D-Link, por lo que los usuarios afectados deben considerar medidas de mitigación o la sustitución del dispositivo.

A. Productos afectados:

- D-Link DIR-880L, versiones de firmware hasta 104WWb01.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//vuldb[.]com/?id.307459 • hxxps[:]//vuldb[.]com/?submit.556433 • hxxps[:]//github[.]com/CH13hh/tmp_store_cc/blob/main/DIR-880L/1.md • hxxps[:]//www[.]dlink[.]com/en

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°105	Fecha: 06-05-2025 Página: 5 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el navegador Chrome de Google		
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:

Google LLC ha publicado una vulnerabilidad de severidad **ALTA** de tipo desbordamiento de búfer de pila que afecta al motor de renderizado HTML de Google Chrome. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto explotar la corrupción de pila mediante una página HTML manipulada.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-4096 de tipo desbordamiento de búfer de pila, podría permitir a un atacante remoto explotar la corrupción de pila mediante una página HTML manipulada. Una explotación exitosa podría tener graves consecuencias, incluyendo la ejecución de código arbitrario, lo que significa que los atacantes podrían obtener el control del sistema.

A. Productos afectados:

- Google Chrome, versiones anteriores a 136.0.7103.59.

3. RECOMENDACIÓN:

- Actualizar Google Chrome a la versión136.0.7103.59 o posterior.

Fuente de Información:	• hxxps[:]//chromereleases[.]googleblog[.]com/2025/04/stable-channel-update-for-desktop_29.html • hxxps[:]//issues[.]chromium[.]org/issues/409911705

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°105	Fecha: 06-05-2025 Página: 5 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Samsung MagicINFO Server		
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:

Samsung ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo recorrido de ruta que afecta a Samsung MagicINFO 9 Server, específicamente en el método getFileFromMultipartFile. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en las instalaciones afectadas sin necesidad de autenticación.

2. DETALLES:

MagicINFO sirve como una solución todo en uno para la gestión de contenido, dispositivos y datos, facilitando la creación, distribución y gestión de visualización remota de contenido para las organizaciones.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-7399 de tipo recorrido de ruta que afecta a Samsung MagicINFO Server, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en las instalaciones afectadas sin necesidad de autenticación. Esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en las instalaciones afectadas de Samsung MagicINFO Server. No se requiere autenticación para explotar esta vulnerabilidad.

La falla específica se encuentra en el método getFileFromMultipartFile. El problema se debe a la falta de validación adecuada de una ruta proporcionada por el usuario antes de usarla en operaciones con archivos. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto de SYSTEM.

Samsung lanzó un parche en agosto de 2024 (versión 21.1050) que corrige esta vulnerabilidad. Sin embargo, los actores de amenazas comenzaron a explotar esta vulnerabilidad en Samsung MagicINFO después de la publicación del código PoC el 30 de abril de 2025.

A. Productos afectados:

- Samsung MagicINFO 9 Server, versiones anteriores a 21.1050.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad. Si no es posible aplicar parches de inmediato, implementar controles estrictos de acceso a la red en los servidores afectados.
- Supervisar los registros del sistema para detectar operaciones sospechosas con archivos, especialmente aquellas que involucren permisos a nivel de sistema.
- Aplicar el principio de mínimo privilegio a todas las cuentas de usuario y servicio.
- Implementar listas blancas de aplicaciones para evitar la ejecución de código no autorizado.
- Auditar periódicamente los permisos y la integridad del sistema de archivos para detectar cambios no autorizados.
- Implementar la segmentación de la red para aislar los sistemas vulnerables si no se pueden aplicar parches de inmediato.

Fuente de Información:	• hxxps://www.zerodayinitiative.com/advisories/ZDI-24-1128/ • hxxps://security.samsungtv.com/securityUpdates • hxxps://talkback.sh/resource/89f094d1-5dcf-4420-b3bf-60d3b19a96d1/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°105	Fecha: 06-05-2025
		Página: 5 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Kibana utilizada con Elasticsearch		
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 contaminación del prototipo que afecta a Kibana, una herramienta de visualización de datos utilizada con Elasticsearch. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el servidor que aloja Kibana.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-25014 de tipo contaminación del prototipo que afecta a Kibana, podría permitir a un atacante remoto no autenticado ejecutar código mediante el envío de solicitudes HTTP especialmente diseñadas a los endpoints de aprendizaje automático y generación de informes de Kibana.

La vulnerabilidad se puede activar de forma remota a través de solicitudes HTTP, lo que la hace explotable a través de la red sin interacción del usuario.

A. Productos afectados:

- Kibana 8.17.6, 8.18.1 y 9.0.1.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que abordan esta vulnerabilidad.
- Deshabilitar el aprendizaje automático o la función de informes, en caso no puedan actualizar la última versión.

Fuente de Información:	• hxxps://discuss.elastic.co/t/kibana-8-17-6-8-18-1-or-9-0-1-security-update-esa-2025-07/377868

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°105	Fecha: 06-05-2025 Página: 5 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en dispositivos ONS NC600 de Optigo 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:

ICS-CERT ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo uso de credenciales codificadas que afecta a equipos ONS NC600 de Optigo Networks. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante establecer una conexión autenticada con las credenciales codificadas y realizar ejecuciones de comandos del sistema operativo.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-4041 de tipo uso de credenciales codificadas que afecta a equipos ONS NC600 de Optigo Networks, podría permitir a un atacante establecer una conexión autenticada con las credenciales codificadas y realizar ejecuciones de comandos del sistema operativo.

Los atacantes con acceso a la red pueden conectarse al servidor SSH del dispositivo usando estas credenciales codificadas, obteniendo acceso no autorizado y la capacidad de ejecutar comandos arbitrarios a nivel del sistema operativo.

En las versiones 4.2.1-084 a 4.7.2-330 de Optigo Networks ONS NC600, un atacante podría conectarse con el servidor ssh del dispositivo y utilizar los componentes del sistema para realizar ejecuciones de comandos del sistema operativo.

A. Productos afectados:

- Optigo Networks ONS NC600, versión 4.2.1-084 a 4.7.2-330.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Utilizar una tarjeta de interfaz de red (NIC) dedicada en la computadora BMS y utilizar la computadora exclusivamente para conectarse a OneView para administrar la configuración de su red OT.
- Configurar un firewall de enrutador con una lista blanca para los dispositivos autorizados a acceder a OneView.
- Conectarse a OneView a través de una VPN segura.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-126-01

Índice alfabético