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

122-2025-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°122	Fecha: 26-05-2025
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Aplicaciones falsas de DigiYatra atacan a usuarios indios para robarles datos financieros		
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		

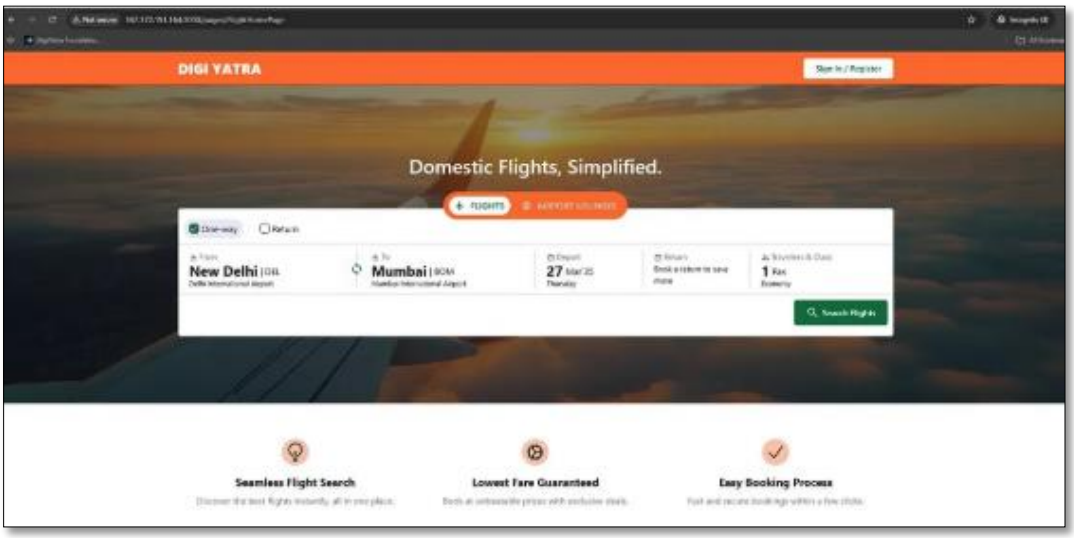
Descripción

1. ANTECEDENTES:

Los actores de amenazas han estado explotando la confianza en la infraestructura pública digital de la India mediante la creación de un sitio de phishing engañoso, digiyatra[.]in, haciéndose pasar por la Fundación DigiYatra.

Este sitio web fraudulento, que todavía estaba activo en el momento del informe, se está utilizando para recopilar datos personales de los usuarios presentándose como un servicio oficial para viajeros aéreos.

El diseño del sitio imita sutilmente un portal de reserva de vuelos legítimo, con un cuadro de búsqueda de vuelos y formularios de usuario que solicitan información personal como nombre, número de teléfono y correo electrónico.



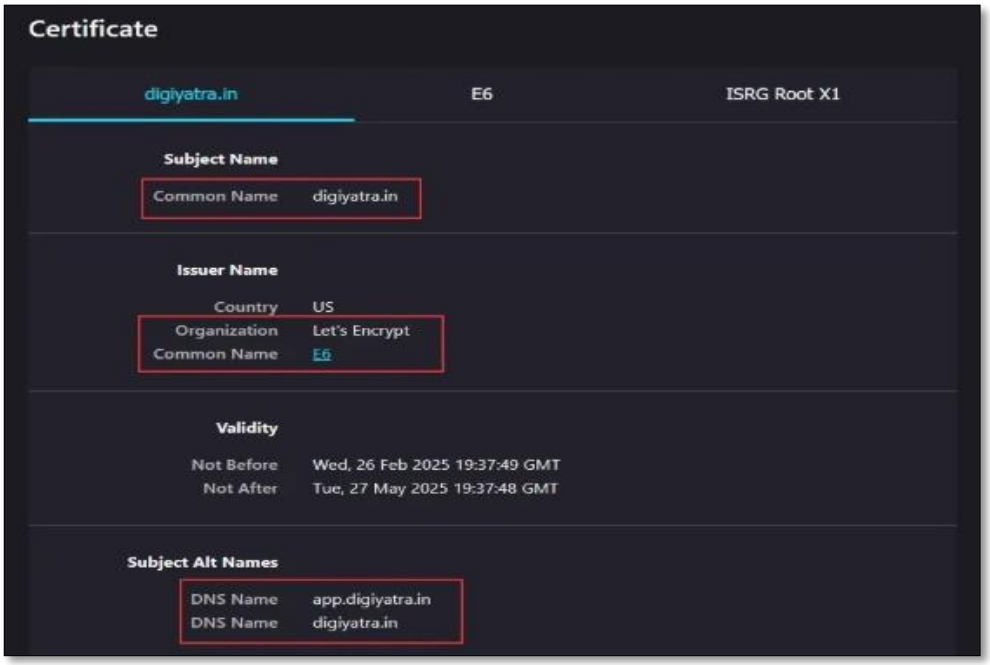
Sin embargo, no se realizan reservas reales y la interfaz está diseñada únicamente para la recopilación de datos. Este diseño engañoso ha sido detectado por el programa de detección temprana de amenazas de ThreatWatch360, que monitorea continuamente los registros de dominios asociados con marcas digitales del sector público como DigiYatra. Tras investigar más a fondo, el equipo descubrió que el sitio utiliza un certificado SSL gratuito de Let's Encrypt, lo que mejora la fachada de legitimidad.

El dominio fue registrado bajo el nombre Ali Sajil de Kerala, India, y a pesar de su naturaleza engañosa, sigue siendo accesible a través de su nombre de dominio y su dirección IP directa (167[.]172[.]151[.]164).

2. DETALLES:

La existencia de este sitio de phishing plantea múltiples amenazas que incluyen, entre otras, la recopilación de datos no autorizada, el engaño público y el posible daño a la reputación de la iniciativa DigiYatra. el verdadero peligro radica en su capacidad de engañar a los usuarios debido al uso de palabras clave y su aparente seguridad (HTTPS). En respuesta, ThreatWatch360 escaló el asunto a CERT-In e inició una solicitud de eliminación con el registrador del dominio. Se han compartido alertas con clientes involucrados en la protección de marca y continúa el monitoreo para detectar intentos fraudulentos similares.

Además, se ha aconsejado bloquear el dominio y su IP a nivel de DNS para evitar más abusos.



Este incidente subraya la importancia de la vigilancia frente a las amenazas cibernéticas, en particular aquellas dirigidas a iniciativas gubernamentales confiables.

Se recomienda a los usuarios que interactúen exclusivamente con el sitio web oficial de la Fundación DigiYatra (hxxps://www[.]digiyatrafoundation[.]com) y que tengan cuidado con los sitios web que suenan o parecen similares, incluso si parecen seguros a través de HTTPS.

Según el informe, se alienta a las organizaciones que brindan servicios digitales públicos a adoptar estrategias proactivas para la protección de la marca y la detección de suplantación de identidad.

En el panorama actual, donde los atacantes frecuentemente explotan nombres que suenan oficiales y marcas confiables, las medidas reactivas ya no son suficientes. Las empresas deben realizar un seguimiento continuo del abuso de dominio, la detección de phishing en tiempo real, el seguimiento de las tergiversaciones de los ejecutivos y una coordinación eficiente con los registradores para la eliminación de sitios. La vigilancia constante de entidades como ThreatWatch360 es crucial para defender la integridad de la infraestructura pública digital.

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos, verificar siempre la URL antes de ingresar datos personales.
- Usar autenticación de dos factores (2FA) agrega una capa extra de seguridad a tus cuentas.
- Revisar errores gramaticales y ortográficos, los correos fraudulentos suelen tener errores evidentes.
- No compartir información personal por correo o mensajes, ninguna entidad legítima te pedirá datos sensibles de esta manera.

Fuente de Información:	• hxxps://gbhackers.com/fake-digiyatra-apps-target-indian-users/ • hxxps://hackread.com/badsuccessor-exploits-windows-server-2025-takeover/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°122	Fecha: 26-05-2025 Página: 6 de 10

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

Canon Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo escritura fuera de límites que genera un desbordamiento de búfer en el procesamiento de autenticación de servicio web en impresoras láser y multifunción Canon para pequeñas oficinas (varios modelos). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante en el segmento de red provocar que el producto afectado no responda (denegación de servicio) o ejecute código arbitrario en el dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-2146 de tipo escritura fuera de límites que genera un desbordamiento de búfer en el componente de autenticación de servicio web en impresoras multifunción Canon Small Office e impresoras láser. La falla se encuentra en el procesamiento de autenticación del servicio web del dispositivo y puede ser explotada por un atacante en el mismo segmento de red. La vulnerabilidad se puede explotar sin autenticación, lo que aumenta el riesgo de explotación generalizada en redes vulnerables.

La explotación exitosa de esta vulnerabilidad podría permitir a un atacante en el segmento de red provocar que el producto afectado no responda (denegación de servicio) o permitir que el atacante ejecute código arbitrario en el dispositivo, lo que podría llevar al compromiso total de la impresora.

A. Productos afectados:

- Japón: Satera MF656Cdw, MF654Cdw, MF551dw, MF457dw (firmware v05.07 y anteriores).
- Estados Unidos: Color imageCLASS MF656Cdw, MF654Cdw, MF653Cdw, MF652Cdw, LBP633Cdw, LBP632Cdw, MF455dw, MF453dw, MF452dw, MF451dw, LBP237dw, LBP236dw, X MF1238 II, X MF1643i II, X MF1643iF II, X LBP1238 II (firmware v05.07 y anteriores).
- Europa: i-SENSYS MF657Cdw, MF655Cdw, MF651Cdw, LBP633Cdw, LBP631Cdw, MF553dw, MF552dw, MF455dw, MF453dw, LBP236dw, LBP233dw, imageRUNNER 1643iF II, 1643i II, i-SENSYS X 1238iF II, X 1238i II, X 1238P II, X 1238Pr II (firmware v05.07 y anteriores).

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de firmware disponible que abordan esta vulnerabilidad.
- Restringir el acceso de la impresora a segmentos de red confiables y evite exponer los dispositivos a redes públicas o no confiables.
- Monitorear el tráfico de red para detectar actividad inusual dirigida a los servicios web de la impresora.

Fuente de Información:	• hxxps://canon.jp/support/support-info/250127vulnerability-response • hxxps://psirt.canon/informacion-advisoria/cp2025-001/ • hxxps://www.canon-europe.com/support/product-security/#news • hxxps://www.usa.canon.com/support/canon-product-advisories/aviso-de-servicio-sobre-medida-de-vulnerabilidad-contra-desbordamiento-de-búfer-para-impresoras-láser-e-impresoras-multifuncionales-de-pequeñas-oficinas

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°122	Fecha: 26-05-2025 Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de omisión de autenticación mediante suplantación de identidad en Siemens SIMATIC IPC RS-828A		
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 omisión de autenticación mediante suplantación de identidad que afecta al servidor de red SIMATIC IPC RS-828A. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir el proceso de autenticación.

2. DETALLES:

SIMATIC IPC (Industrial PC) es la plataforma de hardware para sistemas basados en PC.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-54085 de tipo omisión de autenticación mediante suplantación de identidad en el servidor de red SIMATIC IPC RS-828A, podría permitir a un atacante remoto no autenticado eludir el proceso de autenticación y provocar la pérdida de confidencialidad, integridad o disponibilidad.

La vulnerabilidad se debe a una omisión de autenticación Vulnerabilidad en la interfaz Redfish de su Baseboard Management Controlador (BMC) que podría permitir que un atacante obtenga acceso no autorizado acceder y comprometer la confidencialidad, integridad y disponibilidad de BMC y todo el sistema.

A. Productos afectados:

- SIMATIC IPC RS-828A: Todas las versiones.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://cert-portal.siemens.com/productcert/txt/ssa-446307.txt • hxxps://support.industry.siemens.com/cs/document/109954346 • hxxps://go.ami.com/hubfs/Security%20Advisories/2025/AMI-SA-2025003.pdf • hxxps://security.netapp.com/advisory/ntap-20250328-0003/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°122	Fecha: 26-05-2025 Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el servicio Telnet en dispositivos D-Link DIR-605L y DIR-816L		
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 inyección de comando en el servicio Telnet en D-Link DIR-605L v2.13B01 y DIR-816L v2.06B01. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar comandos arbitrarios de forma remota a través del análisis de firmware.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-46176 de tipo inyección de comando en el servicio Telnet en D-Link DIR-605L v2.13B01 y DIR-816L v2.06B01, podría permitir a un atacante remoto no autenticado ejecutar comandos arbitrarios de forma remota a través del análisis de firmware.

Las credenciales se encuentran analizando el firmware, específicamente una contraseña almacenada en el archivo /etc/alpha_config/image_sign utilizado para el usuario Telnet "Alphanetworks".

El demonio Telnet (telnetd) se inicia con un usuario llamado "Alphanetworks" y una contraseña leída del archivo de firmware image_sign. Esta contraseña está codificada y se puede extraer descomprimiendo y analizando la imagen del firmware del enrutador. Una vez obtenidas las credenciales, un atacante puede iniciar sesión de forma remota a través de Telnet y ejecutar comandos arbitrarios en el dispositivo.

A. Productos afectados:

- D-Link DIR-605L v2.13B01.
- DIR-816L v2.06B01.

3. RECOMENDACIONES:

- Retirar y reemplazar estos dispositivos antiguos con modelos más nuevos y compatibles para mitigar los riesgos de seguridad. D-Link indicó que no hay parches ni actualizaciones de firmware oficiales disponibles para estos dispositivos antiguos afectados, incluidos modelos como el DIR-605L v2.13B01 y el DIR-816L v2.06B01, debido a que han alcanzado el fin de su vida útil (EOL) o el fin de servicio (EOS). D-Link ha cesado el desarrollo de firmware y las actualizaciones de seguridad para estos productos.
- Deshabilitar los servicios Telnet a través de la interfaz de administración.
- Restringir el acceso WAN a los puertos de administración.
- Restringir el acceso del dispositivo únicamente a redes confiables.
- Monitorizar actualizaciones de firmware.
- Supervisar el tráfico de red para detectar conexiones Telnet no autorizadas.

Fuente de Información:	• hxxps://github.com/namberino/cve/tree/main/CVE-2025-46176 • hxxps://www.dlink.com/es/boletin-de-seguridad/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°122	Fecha: 26-05-2025 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Apache Tomcat		
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 equivalencia de ruta: 'file.name' (punto interno) que afecta a múltiples versiones de en Apache Tomcat, un contenedor de servlets Java y servidor web de código abierto ampliamente utilizado. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir los controles de seguridad, lo que lleva a la ejecución remota de código (RCE), la divulgación de información y la inyección de contenido malicioso.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-24813 de tipo equivalencia de ruta que afecta a múltiples versiones de en Apache Tomcat, podría permitir a un atacante remoto no autenticado eludir los controles de seguridad, lo que lleva a la ejecución remota de código (RCE), la divulgación de información y la inyección de contenido malicioso.

Esta vulnerabilidad existe debido a un manejo inadecuado de las rutas de archivos, particularmente aquellas que contienen puntos internos (por ejemplo, file.Name), puede permitir a los atacantes eludir los controles de seguridad, lo que lleva a la ejecución remota de código (RCE), la divulgación de información y la inyección de contenido malicioso.

Si bien se requieren configuraciones específicas, la disponibilidad pública del código de explotación y el escaneo activo hacen que la aplicación rápida de parches y la revisión de la configuración sean fundamentales para todas las implementaciones de Tomcat.

La vulnerabilidad requiere que el servlet predeterminado tenga permisos de escritura habilitados (deshabilitados de manera predeterminada). Las solicitudes PUT parciales deben estar habilitadas (esto normalmente está habilitado de manera predeterminada). Asimismo, la aplicación debe utilizar la persistencia de sesión basada en archivos de Tomcat con la ubicación de almacenamiento predeterminada. La aplicación debe incluir una biblioteca vulnerable a la deserialización.

Un atacante puede explotar la vulnerabilidad cargando una carga útil maliciosa de Java serializada mediante una solicitud PUT al directorio de escritura del servidor. Posteriormente, al enviar una solicitud GET con una JSESSIONIDcookie especialmente diseñada que hace referencia al archivo de sesión cargado, el servidor deserializa la carga útil, lo que desencadena la ejecución de código arbitrario.

A. Productos afectados:

- Apache Tomcat: de 11.0.0-M1 a 11.0.2, de 10.1.0-M1 a 10.1.34 y de 9.0.0.M1 a 9.0.98.

3. RECOMENDACIÓN:

- Actualizar las versiones afectadas a las versiones 11.0.3, 10.1.35 y 9.0.99 o a versiones posteriores, para protegerse contra la explotación, según lo que Apache Tomcat ha publicado.

Fuente de Información:	• hxxps://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq • hxxps://access.redhat.com/security/cve/cve-2025-24813 • hxxps://gbhackers.com/apache-tomcat-rce-vulnerability/ • hxxps://www.cisa.gov/known-exploited-vulnerabilities-catalog

Índice alfabético