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

023-2025-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°023	Fecha: 28-01-2025
		Página: 4 de 11

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Ransomware ataca ESXi a través de túneles SSH ocultos		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

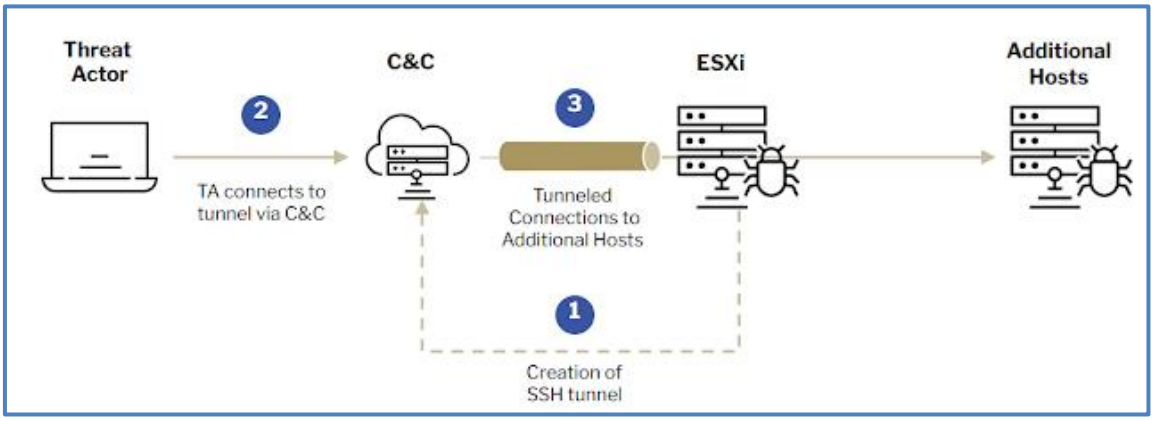
Grupos de ransomware y actores de amenazas están utilizando técnicas de "vivir fuera de la tierra" y utilizando herramientas nativas como SSH para establecer un túnel SOCKS entre sus servidores C2 y el entorno comprometido.

2. DETALLES:

Los investigadores de ciberseguridad han descubierto que los ataques de ransomware dirigidos a sistemas ESXi también aprovechan el acceso para reutilizar los dispositivos como un conducto para canalizar el tráfico hacia la infraestructura de comando y control (C2) y permanecer bajo el radar.

Los dispositivos ESXi, que no están monitoreados, son cada vez más explotados como mecanismo de persistencia y puerta de acceso para acceder ampliamente a las redes corporativas. De esta manera, se integran en el tráfico legítimo y establecen una persistencia a largo plazo en la red comprometida con poca o ninguna detección por parte de los controles de seguridad.

"Dado que los dispositivos ESXi son resistentes y rara vez se apagan inesperadamente, esta tunelización actúa como una puerta trasera semipersistente dentro de la red", señalaron los investigadores de Sygnia Aaron.



3. RECOMENDACIONES:

- Configurar el reenvío de registros de ESXi para capturar todos los eventos relevantes en un solo lugar para las investigaciones forenses.
- Revisar los cuatro archivos de registro siguientes, para detectar ataques que impliquen el uso de túneles SSH en dispositivos ESXi:
  - /var/log/shell.log (ESXi shell activity log)
  - /var/log/hostd.log (Host agent log)
  - /var/log/auth.log (authentication log)
  - /var/log/vobd.log (VMware observer daemon log)

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2025/01/ransomware-ataca-esxi-traves-de-tuneles.html • hxxps://thehackernews.com/2025/01/ransomware-targets-esxi-systems-via.html

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°023	Fecha: 28-01-2025
		Página: 5 de 11

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	28 enero: Día internacional de la protección de datos		
Tipo de Ataque	Divulgación no autorizada de información personal	Abreviatura	DivNoActInfoPer
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	A	Código de Sub familia	A02
Clasificación temática familia	Acceso no autorizado		

Descripción

1. ANTECEDENTES:

En 2006, el Comité de ministros del Consejo de Europa decidió designar el 28 de enero como Día Internacional de la Protección de Datos. En la actualidad, este día se celebra en todo el mundo con el nombre de "Día Internacional de la Protección de Datos" o "Día de la Privacidad". Esta fecha busca concientizar sobre la necesidad de proteger la información personal y empresarial en un mundo hiperconectado.

2. DETALLES:

Los datos personales son cualquier información que puede identificar a una persona, como su nombre, dirección, número de teléfono o sus datos financieros. Su filtración o manejo inadecuado puede llevar a violaciones de privacidad y a la exposición a riesgos como el fraude y la discriminación.

La protección de los datos personales está en el centro de una gobernanza democrática de los datos, lo que nos permitirá avanzar hacia tecnologías más responsables y éticas para el bien común.

El año pasado, el Perú sufrió una serie de ciberataques a instituciones educativas y financieras, lo que provocó la filtración de datos personales de miles de ciudadanos.

Como respuesta a estos incidentes, el gobierno, a finales de noviembre de 2024, publicó el nuevo Reglamento de la Ley N.º 29733, la cual entrará en vigor a fin de marzo, con el objetivo de fortalecer la protección de los datos personales en el país e imponer sanciones severas a las empresas responsables. En caso de incumplimiento, las empresas podrían enfrentar una multa de hasta 535.000 soles (100 UIT).

La Autoridad Nacional de Protección de Datos Personales (ANPDP) será responsable de supervisar y fiscalizar el cumplimiento de esta normativa.

Una de las principales disposiciones es la obligación de notificar a la ANPDP en caso de cualquier incidente de seguridad, como filtraciones o violaciones de datos personales, dentro de las 48 horas siguientes a la detección del incidente.

La notificación debe contener detalles precisos sobre la naturaleza del evento, los tipos de datos comprometidos y el número estimado de personas afectadas.

También se debe informar sobre las posibles consecuencias del incidente y las medidas adoptadas para mitigar la filtración. Si la filtración afecta directamente a los titulares, la empresa debe comunicarles la situación en el mismo plazo.

El reglamento también exige la designación de un Oficial de Datos Personales (DPO) en cada organización, encargado de asegurar el cumplimiento de las normativas de protección de datos y la correcta gestión de la información, conforme a la legislación vigente.

Tiene la responsabilidad de asesorar al responsable del tratamiento de datos y a los empleados encargados de este proceso, asegurando el cumplimiento de las normativas de protección de datos.

Además, se establece la obligación de contar con un documento de seguridad que detalle las políticas y medidas adoptadas para proteger la información personal, asegurando el cumplimiento de las mejores prácticas en ciberseguridad.

3. RECOMENDACIONES:

- Planear escenarios de riesgo y adoptar anticipadamente las medidas de seguridad que corresponda.
- Designar un Oficial de Datos Personales en todas aquellas entidades que hagan tratamiento de grandes volúmenes de datos o traten datos sensibles como actividad principal o giro de negocio (datos de salud, biométricos, afiliación sindical, datos neuronales, entre otros).
- Cumplir con la legislación vigente y colaborar con la ANPDP en su proceso de supervisión.
- Implementar políticas de seguridad claras que regulen el uso adecuado de los recursos tecnológicos y la protección de la información.
- Monitorear la infraestructura tecnológica implementando herramientas que detecten actividades sospechosas y permitan respuestas rápidas frente a posibles amenazas.
- Habilitar la protección de firewall para monitorear y controlar el tráfico de red entrante y saliente.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Programar copias de seguridad periódicas y automáticas de la información crítica y almacenarlas en ubicaciones seguras usando la estrategia 3-2-1-1-0 de copias de seguridad, que consiste en realizar tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube; además que una de las copias esté disponible fuera de conexión, y cero copias sin verificar o con errores.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://www.infobae.com/peru/2025/01/29/empresas-en-peru-enfrentaran-sanciones-de-hasta-535-mil-soles-por-filtracion-de-datos-personales-que-hacer-ante-ciberataques/ • hxxps://www.gob.pe/institucion/minjus/noticias/1067368-ejecutivo-aprueba-nuevo-reglamento-de-la-ley-de-proteccion-de-datos-personales • hxxps://www.coe.int/en/web/data-protection/data-protection-day • https://telefonica.com.pe/dia-proteccion-datos-claves-fortalecer-ciberseguridad-pymes/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°023	Fecha: 28-01-2025 Página: 7 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades en el motor JavaScript V8 de Google Chromium		
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 ha publicado dos vulnerabilidades de severidad **ALTA** de tipo desbordamiento de búfer y acceso a la memoria fuera de los límites en el motor JavaScript V8 de Google Chromium en las plataformas Windows, Mac y Linux. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código arbitrario, provocar una denegación de servicio (DoS) al corromper objetos de memoria y comprometer el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-0611 de tipo desbordamiento de búfer en Google Chromium, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un error de límite en V8 en Google Chrome. Un atacante remoto puede engañar a la víctima para que visite una página web especialmente diseñada, provocar una corrupción de memoria y ejecutar código arbitrario en el sistema. Esta vulnerabilidad permite la corrupción de objetos, que podría ser explotada por un atacante remoto a través de una página HTML especialmente diseñada, lo que podría provocar una corrupción del montón.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-0612 de tipo acceso a la memoria fuera de los límites en el motor JavaScript V8 de Google Chromium, podría permitir a un atacante la ejecución remota de código y obtener el control de los sistemas afectados. Los atacantes pueden explotar esta vulnerabilidad de forma remota sin necesidad de autenticación. El acceso a la memoria fuera de los límites en la versión 8 de Google Chrome anterior a la 132.0.6834.110 permitió que un atacante remoto explotara potencialmente la corrupción del montón a través de una página HTML diseñada.

A. Productos afectados:

- Google Chromium: 132.0.6834.0 - 132.0.6834.109.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión 132.0.6834.110 o posterior que abordan estas vulnerabilidades.
- Supervisar periódicamente los avisos de seguridad de fuentes confiables para obtener actualizaciones sobre vulnerabilidades y parches.
- No hacer clic en enlaces desconocidos ni descargar archivos de fuentes no confiables hasta que hayan actualizado sus navegadores.
- Realizar copias de seguridad periódicas de los datos críticos en ubicaciones seguras y fuera de línea. Esto es fundamental para la recuperación en caso de un ataque exitoso.
- Limitar el acceso a sistemas sensibles solo al personal autorizado para reducir el impacto potencial en caso de un ataque exitoso.
- Utilizar soluciones confiables y mantén su actualización para detectar y eliminar amenazas antes de que causen daños.
- Implementar sistemas que detecten comportamientos sospechosos y establezcan protocolos claros para responder a incidentes.

Fuente de Información:	• hxxps://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop_22.html • hxxps://crbug.com/386143468 • hxxps://issues.chromium.org/issues/386143468 • hxxps://issues.chromium.org/issues/385155406

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°023	Fecha: 28-01-2025 Página: 8 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Actualización de IBM Robotic Process Automation con Automation Anywhere para Spring Framework		
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:

IBM ha publicado una actualización que corrige una vulnerabilidad **CRÍTICA** denominada "Spring4Shell" de tipo inyección de código que afecta a IBM Robotic Process Automation con Automation Anywhere para Spring Framework. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2022-22965 de tipo inyección de código que afecta a IBM Robotic Process Automation con Automation Anywhere, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad existe debido a una validación de entrada incorrecta. Un atacante remoto puede enviar una solicitud HTTP especialmente diseñada a la aplicación afectada y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable. Esta vulnerabilidad viene siendo explotado activamente en la naturaleza.

La vulnerabilidad Spring4Shell representa un riesgo de seguridad significativo para las aplicaciones que utilizan Spring Framework en configuraciones específicas. Las organizaciones que utilizan versiones afectadas deben priorizar las actualizaciones e implementar las mejores prácticas de seguridad para proteger sus sistemas contra posibles ataques.

A. Productos afectados:

- IBM Robotic Process Automation con Automation Anywhere: anterior a la versión 19.0.0.10.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Actualizar Spring Framework a las versiones 5.3.18 o posteriores y 5.2.20 o posteriores.
- Actualizar y utilizar las versiones 10.0.20, 9.0.62 o 8.5.78 de Apache Tomcat para obtener capas de protección adicionales.

Fuente de Información:	• hxxp://lab.wallarm.com/update-on-0-day-vulnerabilities-in-spring-spring4shell-and-cve-2022-22963/ • hxxp://tanzu.vmware.com/security/cve-2022-22965 • hxxp://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°023	Fecha: 28-01-2025 Página: 9 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en productos 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 múltiples vulnerabilidades de severidad **ALTA** de tipo escritura fuera de límites que afectan a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

Canon es una compañía especializada en productos ópticos, de captura y reproducción de imágenes, que incluye fotografía, vídeo, fotocopiadoras e impresoras.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-12647 de tipo desbordamiento de búfer en el procesamiento de descarga de fuentes CPCA de impresoras multifunción de oficinas pequeñas e impresoras láser, podría permitir a un atacante remoto en el segmento de red active el producto afectado que no responde o ejecute código arbitrario en el sistema de destino.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-12648 de tipo desbordamiento de búfer en el procesamiento de etiquetas EXIF de datos TIFF de impresoras multifunción de oficinas pequeñas e impresoras láser, podría permitir a un atacante en el segmento de red active el producto afectado que no responde o que ejecute código arbitrario en el sistema de destino.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-12649 de tipo desbordamiento de búfer en el procesamiento de fuentes de datos XPS de impresoras multifunción de oficinas pequeñas e impresoras láser, podría permitir a un atacante remoto en el segmento de red active el producto afectado que no responde o que ejecute código arbitrario en el sistema de destino.

A. Productos afectados:

- Color imageCLASS LBP632CDW: 05.04.
- Color imageCLASS LBP633CDW: 05.04.
- Color imageCLASS MF652CW: 05.04.
- Color imageCLASS MF653CDW: 05.04.
- Color imageCLASS MF654CDW: 05.04.
- Color imageCLASS MF656CDW: 05.04.
- i-SENSYS MF657Cdw: 05.04.
- i-SENSYS MF655Cdw: 05.04.
- i-SENSYS MF651Cw: 05.04.
- i-SENSYS LBP633Cdw: 05.04.
- i-SENSYS LBP631Cw: 05.04.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.usa.canon.com/support/canon-product-advisories/service-notice-regarding-vulnerability-measure-against-buffer-overflow-for-laser-printers-and-small-office-multifunctional-printers • hxxps://www.canon-europe.com/support/product-security/#news

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°023	Fecha: 28-01-2025 Página: 10 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Microsoft Internet Explorer		
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:

Microsoft Corporation ha publicado una vulnerabilidad de severidad **ALTA** de tipo ejecución remota de código en la forma en que el motor de scripting maneja los objetos en la memoria en los navegadores de Microsoft. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario del sistema operativo en el dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2019-1005 de tipo ejecución remota de código en la forma en que el motor de scripting maneja los objetos en la memoria en los navegadores de Microsoft, podría permitir a un atacante remoto no autenticado ejecutar comandos arbitrarios del sistema operativo en el dispositivo afectado.

La vulnerabilidad existe debido a un error de límite al procesar contenido HTML dentro del motor de scripting. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, provocar daños en la memoria y ejecutar código arbitrario en el sistema de destino. Un atacante remoto no autenticado puede ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

A. Productos afectados:

- Microsoft Internet Explorer: 9 – 11.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-1005

Índice alfabético