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

120-2025-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°120	Fecha: 23-05-2025
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	184 millones de contraseñas filtradas en texto plano		
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:

El reciente descubrimiento de un enorme contrabando con 184 millones de registros, incluidos nombres de usuario de Apple, Facebook y Google, así como credenciales de cuentas conectadas a varios gobiernos, subraya los riesgos de recopilar imprudentemente información sensible en un repositorio que podría convertirse en un único punto de fallo.

2. DETALLES:

El investigador Bob Dyachenko, junto al equipo de CyberNews, ha encontrado esta filtración masiva alojada en un servidor sin protección alguna, exponiendo credenciales de todo el mundo.

El registro incluye 184.162.718 credenciales de acceso únicas y pesa más de 47 GB. La información no solamente abarca servicios o plataformas de uso diario para el común de las personas, como pueden ser Gmail, Outlook, Apple, Discord, PayPal o WordPress. También presenta datos de logueo a plataformas de sanidad, cuentas financieras, bancos e infraestructuras gubernamentales y educativas de múltiples países.

A diferencia de otras brechas de datos donde las contraseñas suelen estar cifradas, en este caso las contraseñas están completamente legibles, sin ningún tipo de protección. Esto significa que los ciberdelincuentes pueden utilizarlas directamente para:

- Realizar ataques de relleno de credenciales (credential stuffing).
- Acceder a cuentas corporativas y personales.
- Robar información confidencial o suplantar la identidad de empleados.
- Lanzar ataques internos usando accesos legítimos.

Respecto del método usado para la extracción de las contraseñas y credenciales de acceso filtradas, el investigador Jeremiah Fowler, un experto en ciberseguridad, explica que hay señales del uso de infostealers. Se trata de un tipo de software malicioso que suele infectar dispositivos a través de software pirata o campañas de suplantación de identidad (phishing). Este tipo de malware puede obtener la información sensible almacenada en navegadores web, clientes de correo o plataformas de mensajería.

Fowler, quien no descargó los datos, afirma que se puso en contacto con una muestra de las direcciones de correo electrónico expuestas, y que algunas respondieron confirmando que eran cuentas auténticas.

3. RECOMENDACIONES:

- Verificar si tus cuentas han sido comprometidas.
- Cambiar las contraseñas de todas sus cuentas de manera periódica utilizando una contraseña fuerte y única para cada sitio.
- Habilitar la autenticación de dos factores en toda aplicación que esté disponible.
- Considerar utilizar un gestor de contraseñas para mantener tus credenciales seguras y fáciles de administrar.
- Auditar los accesos actuales y revisar cualquier actividad inusual en tus sistemas.
- Educar a los usuarios sobre cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://www.infordisa.com/soc/filtracion-de-184-millones-de-contrasenas-esta-tu-empresa-en-riesgo/ • hxxps://blog.segu-info.com.ar/2025/05/184-millones-de-contrasenas-filtradas.html • hxxps://es.wired.com/articulos/el-sueno-de-cualquier-hacker-esta-filtracion-de-184-millones-de-registros-permanece-en-el-misterio

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°120	Fecha: 23-05-2025 Página: 5 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Trimble Cityworks		
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 **ALTA** de tipo deserialización de datos no confiables en Trimble Cityworks. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante autenticado ejecutar código remoto en un servidor web de Microsoft Internet Information Services (IIS). El actor de amenaza de habla china "UAT-6382" están explotando activamente esta vulnerabilidad en la naturaleza.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-0994 de tipo deserialización de datos no confiables en Trimble Cityworks, podría permitir a un atacante autenticado ejecutar código remoto en un servidor web de IIS de Microsoft. Un atacante autenticado con privilegios bajos podría ejecutar código arbitrario en el servidor web IIS vulnerable. Esta vulnerabilidad es de alta gravedad y afecta la confidencialidad, integridad y disponibilidad del sistema. Los atacantes podrían obtener acceso no autorizado, modificar datos del sistema o interrumpir las operaciones del servicio.

Cisco Talos descubrió un ataque de ejecución de código remoto dirigido a la vulnerabilidad CVE-2025-0994 en el sistema de gestión de activos Cityworks. La vulnerabilidad se utilizó para implementar shells de red y malware como Cobalt Strike y VShell, que se cargaron a través de TetraLoader escrito en Rust. La actividad del ataque fue atribuida a actores de amenazas de habla china "UAT-6382".

Las Balizas Cobalt Strike son códigos de shell en memoria e independientes de la posición que TetraLoader inyecta en un proceso benigno específico y VShell stager es un código shell independiente de la posición, que se ha identificado como un stager para VShell, que se comunica con un servidor de comando y control (C2) codificado y ejecuta el código que se le envía.

A. Productos afectados:

- Trimble Cityworks, versiones anteriores a la 23.10.

B. Indicadores de Compromiso (IoC):

TetraLoader:

- 14ed3878b6623c287283a8a80020f68e1cb6bfc37b236f33a95f3a64c4f4611f.
- 4ffc33bdc8527a2e8cb87e49cdc16c3b1480dfc135e507d552f581a67d1850a9.
- 1de72c03927bcd2810ce98205ff871ef1ebf4344fba187e126e50caa1e43250b.
- 1c38e3cda8ac6d79d9da40834367697a209c6b07e6b3ab93b3a4f375b161a901.

Balizas Cobalt Strike:

- C02d50d0eb3974818091b8dd91a8bbb8cdefd94d4568a4aea8e1dcdd8869f738.

IoC de red:

- cdn[.]phototagx[.]com.
- www[.]roomako[.]com.
- lgaircon[.]xyz.
- hxxps://www[.]roomako[.]com/jquery-3[.]3[.]1[.]min[.]js.
- hxxps://lgaircon[.]xyz/owa/OPWiaTU-ZEbuwIAKGPHoQAP006-PTsjBGKQUxZorq2.

- hxxps://cdn[.]lgaircon[.]xyz/jquery-3[.]3[.]1[.]min[.]js.
- hxxps[://]cdn[.]phototagx[.]com/.
- 192 [.]210 [.] 239 [.] 172.
- hxxp[://]192[.]210[.]239[.]172:3219/LVLWPH[.]exe.
- hxxp[://]192[.]210[.]239[.]172:3219/MCUCAT[.]exe.
- hxxp[://]192[.]210[.]239[.]172:3219/TJPLYT[.]exe.
- hxxp[://]192[.]210[.]239[.]172:3219/z44[.]exe.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Restringir el acceso de red al servidor web IIS.
- Implementar mecanismos de autenticación sólidos.
- Supervisar las actividades de red sospechosas.
- Aplicar el principio de mínimo privilegio para las cuentas de usuario.
- Actualizar y aplicar parches regularmente a todos los sistemas.

Fuente de Información:	• hxxps://blog.talosintelligence.com/uat-6382-exploits-cityworks-vulnerability/ • hxxps://unsafe.sh/go-336859.html • hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-037-04 • hxxps://github.com/Cisco-Talos/IOCs/tree/main/2025/05

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°120	Fecha: 23-05-2025 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en la aplicación PrinterShare para Android		
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:

KoreLogic Security ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo exposición de información sensible a un actor no autorizado en la aplicación de impresión móvil PrinterShare para Android que permite la captura no autorizada de tokens de autenticación de Gmail. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado acceder a la cuenta de Gmail de un usuario sin la autorización adecuada.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-5098 de tipo exposición de información sensible a un actor no autorizado en la aplicación de Android PrinterShare que permite la captura no autorizada de tokens de autenticación de Gmail, podría permitir a un atacante remoto no autenticado acceder a la cuenta de Gmail de un usuario sin la autorización adecuada.

Los atacantes pueden capturar tokens de autenticación de Gmail a través de la aplicación. Una vez obtenidos, estos tokens pueden reutilizarse para obtener acceso no autorizado a la cuenta de Gmail de la víctima, lo que podría exponer correos electrónicos confidenciales y datos personales. La vulnerabilidad puede explotarse de forma remota, ya que implica la interceptación o el manejo inadecuado de tokens de autenticación dentro de la aplicación.

A. Productos afectados:

- PrinterShare Mobile Print App para Android: versión 12.15.01.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad; en caso no exista un parche disponible, evitar utilizar la aplicación de Android PrinterShare afectada hasta que se publique una solución.
- Monitorear las fuentes oficiales para obtener actualizaciones o parches de Mobile Dynamix.
- Considerar revocar los permisos de la aplicación y el acceso a Gmail desde la configuración de seguridad de la cuenta de Google.

Fuente de Información:	• hxxps://korelogic.com/Resources/Advisories/KL-001-2025-003.txt

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°120	Fecha: 23-05-2025
		Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en productos IBM		
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 Corporation ha publicado dos vulnerabilidades de severidad **CRÍTICA** de tipo inyección de código y error de validación de entrada que afecta a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema y comprometer la aplicación afectada.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-1302 de tipo inyección de código, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada incorrecta. Un atacante remoto puede ejecutar código arbitrario en el sistema aprovechando el uso inseguro del modo "eval='safe'" por defecto.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-21534 de tipo error de validación de entrada, podría permitir a un atacante remoto comprometer la aplicación afectada. La vulnerabilidad existe debido a una validación insuficiente de la información proporcionada por el usuario. Un atacante remoto puede explotar el uso predeterminado inseguro de vm en Node y ejecutar código arbitrario en el sistema.

A. Productos afectados:

- Watsonx Assistant Cartridge: anteriores a la versión 5.1.3.
- Watsonx Orchestrate with watsonx Assistant Cartridge - Assistant Builder Component: anteriores a la versión 5.1.3.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.ibm.com/support/pages/node/7234091

Índice alfabético