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

101-2025-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°101	Fecha: 30-04-2025
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	La cadena británica Co-op desactiva parcialmente sus sistemas informáticos tras un intento de ciberataque		
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 cadena británica de supermercados Co-op Food ha confirmado a través de un comunicado que ha experimentado una interrupción operativa limitada como resultado de un ciberataque.

La empresa, que opera en más de 2300 tiendas de alimentación en todo el Reino Unido, además de tener negocios de servicios funerarios, jurídicos y de seguros, han indicado que unos piratas informáticos intentaron entrar en sus sistemas, tras un importante ataque contra la cadena de ropa y alimentación Marks & Spencer.

2. DETALLES:

Según la información proporcionada, el ataque causó interrupciones operativas limitadas, lo que sugiere que los sistemas críticos pudieron haber sido aislados o protegidos mediante protocolos de contingencia.

La medida se describió como preventiva y su objetivo era contener la amenaza antes de que los sistemas pudieran verse comprometidos, lo cual suele consistir en aislar segmentos de red afectados, desconectar temporalmente sistemas no esenciales, y activar planes de continuidad del negocio.

Aunque el cierre afectó funciones internas como escritorios virtuales, sistemas de stock y operaciones del centro de contacto, Co-op aseguró al público que todas las tiendas de alimentos, los servicios de entrega a domicilio y las operaciones funerarias funcionan con normalidad.

Afirmó que los datos a los que se había accedido incluían información relativa a un número significativo de sus miembros actuales y antiguos, incluidos datos personales como nombres, datos de contacto y fechas de nacimiento.

Sin embargo, no se han visto afectadas las contraseñas de los miembros, los datos bancarios o de tarjetas de crédito, las transacciones ni la información relacionada con los productos o servicios de los miembros o clientes del grupo.

Posibles vectores de ataque en el sector minorista:

- Sistemas de punto de venta (POS) con vulnerabilidades conocidas.
- Bases de datos que almacenan información de clientes y pagos.
- Cadenas de suministro digitalizadas con múltiples puntos de entrada.
- Infraestructura heredada en algunos casos.

3. RECOMENDACIONES:

- Segmentar redes para restringir el movimiento lateral desde los dispositivos infectados.
- Programar monitoreos continuos mediante soluciones SIEM y XDR.
- Desarrollar planes de respuesta y recuperación ante incidentes, incluyendo pruebas regulares y evaluación de resultados.
- Realizar capacitaciones obligatorias en concienciación sobre seguridad.
- Generar backups inmutables y verificarlos regularmente.

Fuente de Información:	
	• hxxps://enigmasecurity.cl/noticias-1062/ • hxxps://hackread.com/uk-retail-co-op-shuts-down-it-systems-cyberattack/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°101	Fecha: 30-04-2025 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades en el software ThinManager de Rockwell Automation		
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:

Rockwell Automation ha publicado dos vulnerabilidades de severidad **ALTA** de tipo restricción incorrecta de operaciones dentro de los límites de un búfer de memoria y permisos predeterminados incorrectos que afectan a la plataforma de gestión de software ThinManager. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante aumentar los privilegios y provocar una condición de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-3618 de tipo restricción inadecuada de operaciones dentro de los límites de un búfer de memoria, podría permitir a un atacante provocar una condición de denegación de servicio en el software objetivo. El software ThinManager no verifica adecuadamente el resultado de la asignación de memoria al procesar mensajes de tipo 18. Si se explota, un atacante podría provocar una denegación de servicio en el software objetivo.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-3617 de tipo permisos predeterminados incorrectos, podría permitir a un atacante heredar privilegios elevados. Al iniciarse el software ThinManager, se eliminan archivos de la carpeta temporal, lo que provoca que la entrada de control de acceso del directorio herede los permisos del directorio principal. Si se explota, un atacante podría heredar privilegios elevados.

A. Productos afectados:

- ThinManager: versión 14.0.0 y anteriores.

3. RECOMENDACIÓN:

- Actualizar ThinManager a v14.0.2 o posterior para mitigar CVE-2025-3617.

Fuente de Información:	• hxxps://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1727.html • hxxps://support.rockwellautomation.com/app/answers/answer_view/a_id/1085012/loc/en_US#highlight

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°101	Fecha: 30-04-2025 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Azure Machine Learning de Microsoft		
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:

Corporación Microsoft ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo autorización indebida que afecta a Azure Machine Learning. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante autorizado elevar privilegios en una red.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-30390 de tipo autorización indebida que afecta a Azure Machine Learning, podría permitir a un atacante autorizado elevar privilegios en una red.

Un atacante con acceso a la red de bajo nivel podría obtener privilegios de alto nivel no autorizados en el entorno de Azure Machine Learning, comprometer la confidencialidad del sistema al acceder a información confidencial, modificar o interrumpir la integridad del sistema y afectar la disponibilidad del sistema.

A. Productos afectados:

- Azure Machine Learning.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Revisar y restringir el acceso a la red.
- Implementar controles de acceso con privilegios mínimos.
- Supervisar intentos sospechosos de escalada de privilegios.
- Validar y actualizar las configuraciones de Azure Machine Learning.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-30390

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°101	Fecha: 30-04-2025
		Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de desbordamiento de búfer basado en montón en Windows y Windows 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:

Microsoft Corporation ha publicado una vulnerabilidad de severidad **MEDIA** de tipo desbordamiento de búfer basado en montón en Windows y Windows Server. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto autenticado aumentar privilegios en el sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-26634 de tipo desbordamiento de búfer basado en montón en Windows y Windows Server, podría permitir a un atacante remoto no autenticado aumentar privilegios en el sistema.

La vulnerabilidad existe debido a un error de límite en Windows Core Messaging. Un usuario remoto puede enviar una solicitud especialmente diseñada al sistema, provocar un desbordamiento de búfer basado en el montón y ejecutar código arbitrario con privilegios de SYSTEM.

A. Productos afectados:

- Windows: 10 21H2 10.0.19041.3920 - 10 21H2 10.0.19044.5371, 10 22H2 10.0.19041.3920 - 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.1643 - 10 1507 10.0.10240.20890, 10 1607 10.0.14393.10 - 10 1607 10.0.14393.7699, 10 1809 10.0.17763.1 - 10 1809 10.0.17763.6775, 11 22H2 10.0.22449.1000 - 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.1825 - 11 23H2 10.0.22631.4751, 11 24H2 10.0.26052.1000 - 11 24H2 10.0.26100.3107.
- Windows Server: 2008 R2 SP1 - 2008 R2 6.1.7601.27618, 2016 10.0.14393.10 - 2016 10.0.14393.7699, 2019 10.0.17763.1 - 2019 10.0.17763.6775, 2022 10.0.20348.202 - 2022 23H2 10.0.25398.1369, 2025 10.0.26100.1742 - 2025 10.0.26100.3107.

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/vulnerability/CVE-2025-26634

Índice alfabético