



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

059-2026-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 Aérea del 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 las empresas 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

Microsoft confirma el problema de advertencia de Escritorio remoto tras la actualización de abril. 4

Actividad del Trígona ransomware incorpora herramienta personalizada para exfiltración sigilosa de datos y evasión de controles de seguridad. 6

Vulnerabilidad crítica de ejecución remota de código en Apache MINA. 9

Índice alfabético 10

 Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 059		Fecha: 27-04-2026
			Página: 4 de 10
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Microsoft confirma el problema de advertencia de Escritorio remoto tras la actualización de abril.		
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 confirmó una incidencia de seguridad posterior a la actualización de abril de 2026 para Windows 11 (versión 26H1), relacionada con el Protocolo de Escritorio Remoto (RDP). Esta situación surge como consecuencia de los esfuerzos de endurecimiento de seguridad implementados por Microsoft tras detectarse campañas activas de phishing que abusaban de archivos .rdp manipulados para engañar a los usuarios y obtener acceso no autorizado a recursos locales. Dichas campañas fueron alertadas previamente por organismos de ciberseguridad, como el NCSC del Reino Unido, debido a vulnerabilidades de suplantación que permitían ocultar la procedencia real de las conexiones remotas.

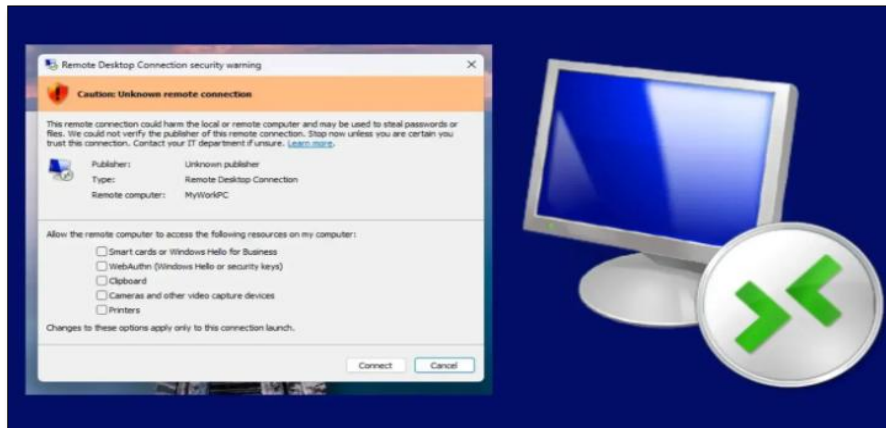


Ilustración 1 Microsoft confirma el problema de advertencia de Escritorio remoto tras la actualización de abril.

2. DETALLES:

La actualización de abril incorporó nuevas advertencias de seguridad en la aplicación de Conexión a Escritorio Remoto (MSTSC), con el objetivo de mostrar alertas más claras y deshabilitar por defecto la redirección de recursos locales (portapapeles, discos y dispositivos).

No obstante, Microsoft reconoció un error de interfaz gráfica que provoca que estas advertencias se muestren de forma incorrecta, con textos superpuestos y botones parcialmente ocultos.

Este fallo impide a los usuarios revisar adecuadamente la información de seguridad y aceptar o rechazar la conexión de manera consciente.

El problema se manifiesta principalmente en entornos con múltiples monitores y configuraciones de escalado de pantalla diferentes, afectando la interacción segura con RDP.

Aunque no se trata de una vulnerabilidad explotable directamente, sí reduce la efectividad de las protecciones antifraude introducidas y puede incrementar el riesgo de errores humanos.


Microsoft trabaja en una corrección definitiva y ha documentado mitigaciones temporales para entornos empresariales.

3. RECOMENDACIONES:

- Restringir el uso de RDP expuesto a Internet, permitiendo accesos únicamente a través de VPN seguras y autenticadas.
- Aplicar autenticación multifactor (MFA) en todos los accesos remotos para reducir el impacto del robo de credenciales.
- Bloquear la apertura automática de archivos .rdp provenientes de correos electrónicos o fuentes no confiables.
- Deshabilitar la redirección de recursos locales (discos, portapapeles, USB) salvo cuando sea estrictamente necesario.
- Mantener los sistemas actualizados y monitorear los boletines oficiales de Microsoft para aplicar parches correctivos tan pronto estén disponibles.
- Capacitar a los usuarios en la identificación de intentos de phishing que utilicen accesos remotos como vector inicial.
- Implementar monitoreo y registros (logging) de sesiones RDP, con alertas ante comportamientos anómalos.
- Usar listas blancas de direcciones IP y políticas de acceso condicional para conexiones remotas críticas.

Fuente de Información:

- <https://gbhackers.com/microsoft-confirms-remote-desktop-warning-issue/>

	ALERTA DE SEGURIDAD DIGITAL N°231		Fecha: 27-04-2026
			Página: 6 de 10
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Actividad del Trigona ransomware incorpora herramienta personalizada para exfiltración sigilosa de datos y evasión de controles de seguridad.		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros.		
Código de familia	C	Código de Sub familia	C09
Clasificación temática familia	Código malicioso		
Descripción			
<p>1. ANTECEDENTES:</p> <p>Investigadores de Symantec identificaron una evolución relevante del ransomware Trigona, cuyos afiliados han incorporado la herramienta personalizada uploader_client.exe para optimizar la exfiltración de datos en entornos Windows y Linux comprometidos, manteniendo su operatividad pese a intentos de desarticulación en 2023; bajo el modelo RaaS y una estrategia de doble extorsión, el grupo roba información sensible antes de cifrar sistemas y exigir pagos en Monero, destacando el uso de conexiones paralelas, rotación de tráfico TCP y filtrado selectivo para evadir controles EDR/DLP, lo que eleva el impacto a un nivel alto al facilitar el robo masivo de datos, comprometer la confidencialidad, integridad y disponibilidad, y generar riesgos significativos como sanciones regulatorias, daño reputacional y pérdidas financieras.</p> <p>Cabe indicar que Los ciberdelincuentes están pirateando servidores Microsoft SQL públicos y con poca seguridad para desplegar el ransomware Trigona.</p>			
<p>2. DETALLES:</p> <p>Trigona es una variante de malware que se descubrió en octubre de 2022, y los investigadores de la Unidad 42 de Palo Alto informaron de similitudes entre Trigona y el ransomware CryLock. Trigona está escrito en lenguaje Delphi, cifra archivos sin distinguir sus extensiones y añade la extensión “._locked” al nombre de los archivos cifrados. Los atacantes lanzan ataques de fuerza bruta o de diccionario contra el servidor en un intento de adivinar las credenciales de la cuenta. Una vez que obtienen acceso al servidor, los ciberdelincuentes despliegan un malware que la empresa de ciberseguridad AhnLab identifica como CLR Shell. CLR Shell permite a los operadores recopilar información del sistema y elevar sus privilegios a LocalSystem explotando una vulnerabilidad en el Servicio de inicio de sesión secundario de Windows.</p> <p>En esta campaña, la cadena de ataque asociada al ransomware Trigona evidencia un modelo maduro de operación tipo Ransomware como servicio (RaaS), caracterizado por una fase inicial orientada a la obtención de acceso persistente en entornos corporativos. Si bien la fuente principal no detalla explícitamente el vector de intrusión en esta variante, el comportamiento histórico del grupo indica el uso de explotación de servicios expuestos, credenciales comprometidas o acceso remoto mediante herramientas legítimas. Una vez dentro del entorno, los atacantes priorizan la estabilidad del acceso mediante la instalación de software de administración remota como AnyDesk, lo que les permite mantener control continuo sin levantar alertas inmediatas en sistemas tradicionales de monitoreo.</p> <p>Posteriormente, el actor ejecuta una fase intensiva de evasión de defensas (Defense Evasion), la cual constituye uno de los elementos más sofisticados de esta campaña. En esta etapa, se emplean herramientas especializadas que operan a nivel de kernel mediante la técnica BYOVD (Bring Your Own Vulnerable Driver). El uso del driver HRSword permite deshabilitar o terminar procesos asociados a soluciones de seguridad como EDR y antivirus. Complementariamente, herramientas como PCHunter, GMER y WkTools facilitan la manipulación de procesos y la inspección profunda del sistema, mientras que utilidades como PowerRun permiten la ejecución de código con privilegios elevados. Esta combinación reduce significativamente la capacidad de detección basada en comportamiento y firmas.</p> <p>Una vez asegurado el entorno, los atacantes avanzan hacia la fase de recolección de credenciales y movimiento lateral. Para ello, emplean herramientas ampliamente conocidas como Mimikatz y utilidades de Nirsoft, orientadas a la extracción de credenciales almacenadas en memoria o en el sistema. Este proceso permite escalar privilegios y expandirse dentro de la red comprometida, accediendo a sistemas críticos y repositorios de información sensible. La reutilización de credenciales válidas facilita además eludir controles de autenticación tradicionales, consolidando el dominio del atacante sobre la infraestructura afectada.</p> <p>La fase más relevante en esta evolución de Trigona corresponde a la exfiltración de datos, donde se introduce una herramienta personalizada denominada uploader_client.exe. Este componente ha sido diseñado específicamente para maximizar la eficiencia y el sigilo durante la extracción de información. La herramienta establece múltiples conexiones paralelas (hasta cinco por archivo), lo que acelera significativamente la transferencia de datos hacia servidores controlados</p>			

por el atacante. Además, implementa rotación de conexiones TCP cada 2 GB transferidos, dificultando la correlación de eventos en soluciones de monitoreo de red. Asimismo, incluye mecanismos de filtrado para excluir archivos de bajo valor (como contenido multimedia), enfocándose en documentos sensibles como PDFs, bases de datos y registros financieros. La autenticación mediante claves preconfiguradas y el uso de direcciones de servidor hardcodedas refuerzan el control sobre la infraestructura de exfiltración.

Finalmente, tras completar la extracción de información, el ataque culmina con el despliegue del payload de ransomware, ejecutando el cifrado de los sistemas comprometidos. Esta etapa está alineada con el modelo de doble extorsión, donde los atacantes no solo bloquean el acceso a la información, sino que también amenazan con publicar los datos previamente exfiltrados en caso de no recibir el pago exigido. Este enfoque incrementa significativamente la presión sobre las víctimas, combinando impacto operativo con riesgo reputacional y regulatorio. En conjunto, la cadena de ataque demuestra una clara priorización de la exfiltración como fase crítica, marcando una evolución hacia operaciones más silenciosas, dirigidas y efectivas en la monetización del acceso comprometido.

A. Vulnerabilidades explotadas:

- CVE-2021-40539 – Authentication Bypass / RCE en ManageEngine ADSelfService Plus.

B. Indicadores de Compromiso (IoC):

- 0b679027e38f3d9ca554085be0e762c651e83e6414401b56635cdf3765ca1dac – AnyDesk,
- 0ce7badb26174b6129fb13d7e255e582f84d8aaedeabcd02c80d84a609144068 – PCHunte,
- 1433aa8210b287b8d463d958fc9ceeb913644f550919cfb2c62370773799e5a5 - Controlador vulnerable (wktools.sys),
- 1588023393eb6b4d9433d539d303ecb56b6c3630e860f94d1a137834bdebf2bd – PCHunter,
- 205818e10c13d2e51b4c0196ca30111276ca1107fc8e25a0992fe67879eab964 - Escritorio remoto PassView,
- 207b11f7dc4f17e4e5a9c25dbfb6a785a7456d7c381ecea7c729d8d924be1fb9 – PCHunter,
- 274ca13168b38590c230bddc2d606bbe8c26de8a6d79156a6c7d07265efe0fdf – PCHunter,
- 2b214bddaab130c274de6204af6dba5aeec7433da99aa950022fa306421a6d32 – PCHunter,
- 35f28a31a47b0bcd92722265473d66ffef6c4bd460c71c36b57df2ac0d02f671 – MalExtractor,
- 396aa1f8f308010a3c76a53965d0eddd35e41176eacd1194745d9542239ca8dc – Cargador,
- 4a44d0c6cf5de515dd296f05ff6674d1a340fccf6b4c11612d27be2d3baa82b0 – PCHunter,
- 4adbb1906762c757764ffc5fa64af96e091966f4f5a43aae12fcc4f05f1c26b5 - Monitor de procesos StpBYOVD,
- 598555a7e053c7456ee8a06a892309386e69d473c73284de9bbc0ba73b17e70a - Contraseña de acceso telefónico,
- 5be325905df8aab7089ab2348d89343f55a2f88dadd75de8f382e8fa026451bd – Mailpassview,
- 6688fb3039ad6df606d76a897ef1072cdc78b928335c6bfa691d99498caf5c4b – Mimikatz,
- 6bac99f56e54d5195783513ae6954a4a8509d7bc397c94f405266b5df9cd96cb – ParsVbs,
- 6ce228240458563d73c1c3cbbd04ef15cb7c5badacc78ce331848f5431b406cc – HRSword,
- 72fc3d03065922b9a03774bbd1873e5e7f3a5a2abf5dcf7bfb2e98aced53a9d – AnyDesk,
- 73cd405b5bfc99ec5cf33467d4be7fc7e39ae18337568ee10173c17ba6e8f0d7 – AnyDesk,
- 771de264c5d7e1e5ac85f00c42e9fe3b439bcbdf9aa11e4fd7bc0d87fa2344e – MalExtractor,
- 7a313840d25adf94c7bf1d17393f5b991ba8baf50b8cacb7ce0420189c177e26 - Contraseña de Messenger,
- 816d7616238958dfe0bb811a063eb3102efd82eff14408f5cab4cb5258bfd019 – VNCPassView,
- 87bf4b152d9548f415f12f353f988b5442729e7f24e2902dfd0baa4a944354a – DumpGuard,
- 8a2f4907159a68867b22bc772590ebcafca656a23951228ecd89e4f598472b0 – DumpGuard,
- b066ca2702853c2fcbf686897c18f6d315be7ae753007ac2c1d73c87b0a30de9 – PowerRun,
- b3774ba01a3096348fd76a7072407b9f07bb9589e0f5ba31ca576689bbbe94e4 – HRSword,
- c41216eee9756a1dcc546df4fe97defc05513eed64ce6ac05f1501b50e6f96cc - Vista de contraseña del navegador web,
- c64964944b4c1f649ae8f694964b3a212dc1028341ab71836306a456fba0b3f4 - Controlador vulnerable (ke64.sys),
- c7d994eb2042633172bd8866c9f163be531444ce3126d5f340edd25cbdb473d4 – NetScan,
- d4339a5b9d15211dbc85424cf7fa8ff825033ea3378506d8ecb19b016db5b4ff – Yoscurio,
- d833e8fc97b3c865ebfb96a48da9ec446148cb5ad7e66ca5c47cd693f7923888 - AnyDesk,
- df5a574254637d2880633b0582e956b23f66efc6781e825c65e1ccfaa6c58809 – StartBat,
- e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173 – Gmer,
- eee885e5dae750848d0903d179cacd81149ceec83c2ec4ad4545531de3cfd – HRSwordExtractor,
- f27eab3157451e31db71169e71f76d28325193218f9dc8f421136d4a20165feb – WKTools,
- 48f3d66492a494965e7039079158e2fee552aaab517d1a55352209c9eedcb765 - Archivo sospechoso,
- 49a7b3cf426d1f35a2138c0a6cec397688d223d7f2bcbbeed53b511a328a97be – CommandTxt,
- 647b2f12486343fe065dc4abbb11e2338589eb099c72792b5a05e64a5e2937fc – YdarkDriver,
- 6c31dd44b29b5f87030caeeccc616cf366badeff5a7e4c9933aa5fa6445a0c7a - Archivo sospechoso,
- 99c4775ed813f354c9e53f42797226d82b26f44d19e81036c9e55222d1744189 – HRSword,

- a18555c1ca53d4826191a30889d82205a304932f997baec755c98ddad4326cb8 - Archivo sospechoso,
- f5390674f0f49fe8af116396828c3de6729347ebc3c772d87618e55629aec06c – Ydark,
- 163.172.105.82 (Puerto 1080) – Comando y control de exfiltración.

C. Datos clave del incidente:


- Tipo de ataque: Ransomware con doble extorsión,
- Nivel de criticidad: ALTO,
- Organización afectada: No especificada (múltiples víctimas corporativas),
- Productos afectados: Sistemas Windows/Linux empresariales,
- Actor de amenaza: Trigona ransomware (modelo RaaS),
- Impacto: Exfiltración masiva + cifrado + extorsión,
- Fecha del incidente: marzo 2026 (actividad observada).

3. RECOMENDACIONES:

- Implementar monitoreo avanzado de tráfico saliente para detectar volúmenes anómalos de exfiltración y patrones de conexiones paralelas no habituales.
- Desplegar soluciones EDR/XDR con capacidades anti-BYOVD, incluyendo bloqueo de drivers vulnerables y protección a nivel kernel.
- Aplicar listas de control de aplicaciones (Application Allowlisting) para impedir la ejecución de binarios no autorizados como uploader_client.exe.
- Restringir y auditar el uso de herramientas de acceso remoto (AnyDesk, TeamViewer, etc.) mediante políticas de seguridad estrictas.
- Implementar autenticación multifactor (MFA) en accesos privilegiados, servicios expuestos y conexiones remotas.
- Ejecutar rotación periódica de credenciales y aplicar el principio de mínimos privilegios (Least Privilege) en toda la infraestructura.
- Monitorizar el uso de herramientas de dumping de credenciales como Mimikatz y utilidades similares (Nirsoft).
- Deshabilitar o limitar el uso de PowerShell, herramientas administrativas y utilidades de elevación cuando no sean necesarias.
- Fortalecer la segmentación de red para limitar el movimiento lateral entre sistemas críticos.
- Implementar DLP (Data Loss Prevention) para identificar y bloquear transferencias no autorizadas de información sensible.
- Mantener un programa riguroso de gestión de vulnerabilidades, priorizando parches en servicios expuestos a Internet.
- Aplicar hardening del sistema operativo, incluyendo desactivación de servicios innecesarios y protección de memoria.
- Configurar alertas sobre ejecución de drivers no firmados o sospechosos, especialmente asociados a técnicas BYOVD.
- Realizar copias de seguridad (backups) offline e inmutables, verificando periódicamente su integridad y capacidad de restauración.
- Desarrollar y probar planes de respuesta a incidentes (IRP) enfocados en ransomware y exfiltración de datos.
- Capacitar al personal en detección de accesos anómalos y uso indebido de credenciales, especialmente en equipos de TI.
- Correlacionar eventos en un SIEM para identificar comportamientos encadenados (acceso remoto + dumping credenciales + exfiltración).
- Implementar controles de egress filtering para restringir comunicaciones hacia dominios/IPs no autorizados.
- Auditar continuamente logs de autenticación, ejecución de procesos y transferencias de archivos en endpoints críticos.

Fuente de Información:

- <https://securityaffairs.com/191294/cyber-crime/trigona-ransomware-adopts-custom-tool-to-steal-data-and-evade-detection.html>
- <https://www.security.com/threat-intelligence/trigona-exfiltration-custom>
- <https://securityaffairs.com/145036/cyber-crime/trigona-ransomware-targets-microsoft-sql-servers.html>
- <https://www.broadcom.com/support/security-center/protection-bulletin>

	ALERTA DE SEGURIDAD DIGITAL N°232		Fecha: 27-04-2026
			Página: 9 de 10
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica de ejecución remota de código en Apache MINA.		
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			
<p>1. ANTECEDENTES:</p> <p>Apache Software Foundation ha reportado una vulnerabilidad de severidad “CRÍTICA” clasificada como CWE-502: Deserialización de datos no confiables que afecta a Apache MINA. Esta vulnerabilidad permite la ejecución remota de código (RCE) sin autenticación, lo que implica que un atacante puede comprometer completamente la confidencialidad, integridad y disponibilidad del sistema afectado. El riesgo es especialmente alto en aplicaciones que procesan objetos serializados desde fuentes externas, ya que facilita la ejecución arbitraria de código en el servidor.</p> <p>El impacto de esta vulnerabilidad es máximo (CIA triad). La ejecución remota de código permite a un atacante tomar control total del sistema afectado, desplegar malware, exfiltrar información sensible o pivotar hacia otros sistemas en la red. Dado que Apache MINA es un framework de red ampliamente utilizado, el impacto se extiende a múltiples aplicaciones empresariales críticas.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad crítica identificada por MITRE como CVE-2026-41635 se origina en el método AbstractIoBuffer.resolveClass() de Apache MINA. Este método contiene una bifurcación lógica donde, en ciertos casos (clases estáticas o tipos primitivos), no se realiza validación sobre la clase que se está deserializando. Como resultado, se omite completamente la lista de control (allowlist) de clases permitidas, habilitando la carga de clases arbitrarias mediante Class.forName().</p> <p>En el contexto de CVE-2026-41635, esta omisión de validación permite a un atacante suministrar datos serializados maliciosos que, al ser procesados por la función IoBuffer.getObject(), desencadenan la ejecución de código arbitrario en el sistema objetivo. La explotación no requiere privilegios previos ni interacción del usuario, y puede ser realizada de forma remota, lo que amplifica significativamente su criticidad (CVSS 3.1: 9.8).</p> <p>Hasta el momento, no existen evidencias públicas confirmadas de explotación activa en el mundo real ni atribución a actores de amenaza específicos. Tampoco se dispone de un exploit público funcional (PoC) ampliamente difundido. Sin embargo, dada la simplicidad de explotación y la naturaleza de la vulnerabilidad (deserialización insegura), es altamente probable que surjan PoC en el corto plazo tras su divulgación. No puedo confirmar explotación activa en campañas reales al momento de esta respuesta.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – Apache MINA: 2.0.0 ≤ versión ≤ 2.0.27, 2.1.0 ≤ versión ≤ 2.1.10, 2.2.0 ≤ versión ≤ 2.2.5. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Actualizar inmediatamente a versiones corregidas (2.0.28 / 2.1.11 / 2.2.6), • Evitar el uso de IoBuffer.getObject() con datos no confiables, • Implementar controles estrictos de deserialización (allowlist de clases), • Aplicar mecanismos de sandboxing o aislamiento de procesos, • Monitorizar logs en busca de cargas dinámicas de clases inusuales y ejecución anómala de código Java, • Implementar herramientas de detección de comportamiento (EDR/XDR), • Revisar integridad de sistemas potencialmente expuestos. 			
Fuente de Información:		<ul style="list-style-type: none"> • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21515 	

Índice alfabético

Ransomware 6

Explotación de vulnerabilidades conocidas 4,9