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

024-2025-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°024	Fecha: 29-01-2025
		Página: 4 de 14

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Ransomware Makop y Lynx Atacan Organizaciones en América Latina		
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:**

Los operadores del ransomware Makop y el grupo de ransomware como servicio (RaaS) Lynx, están atacando activamente a organizaciones de América Latina, incluidos sectores críticos, volviéndose parte de las amenazas más agresivas en la región.

2. **DETALLES:**

Sobre el ransomware Makop, una vez que infecta un sistema, cifra los archivos y les añade extensiones como ".makop" o ".mkp", dejando a los afectados sin acceso a su información. Y lo peor es que, hasta ahora, no existen herramientas gratuitas para descifrar los archivos bloqueados.

Los ciberdelincuentes detrás de Makop utilizan varias estrategias para colarse en las redes de sus víctimas.

Algunos de los métodos más comunes incluyen:

- **Accesos remotos sin seguridad (RDP expuesto):** Si una empresa tiene servicios de Escritorio Remoto mal configurados, los atacantes pueden aprovecharlos para entrar.
- **Correos electrónicos de phishing:** Envían mensajes falsos con archivos adjuntos maliciosos que, al abrirse, inyectan el ransomware en el sistema.
- **Descargas de torrents y anuncios maliciosos:** Algunas víctimas terminan instalando el malware sin darse cuenta, al descargar software de fuentes no confiables.

Una vez dentro, Makop no actúa solo. Sus operadores cuentan con un arsenal de herramientas, tanto personalizadas como de código abierto, para moverse dentro de la red y asegurarse de que el ataque sea exitoso.

Estas herramientas adicionales le permiten maximizar su impacto, logrando robar credenciales, automatizar tareas maliciosas y mantener la persistencia en el sistema.

Por ejemplo, aprovechan otros ensamblajes .NET personalizados, como PuffedUp, para lograr etapas posteriores de la cadena de ataque. Esta herramienta en particular está diseñada para garantizar la persistencia después del acceso inicial. Se basa en un archivo de configuración de texto ubicado en la misma carpeta, que contiene una o más cadenas de 42 caracteres que se colocarán en el portapapeles del usuario.

El ransomware Lynx, por su parte, opera bajo un modelo de ransomware como servicio (RaaS), lo que significa que cualquiera, con los contactos y los conocimientos adecuados, puede convertirse en afiliado y usar sus herramientas para realizar ataques.

Para facilitarles el trabajo, han desarrollado un panel de control con secciones como "Noticias", "Empresas", "Chats", "Información" y "Filtraciones".

Este sistema permite a los afiliados:

- Seleccionar y administrar a sus víctimas.
- Generar versiones personalizadas del ransomware.
- Coordinar la filtración de datos en caso de que las víctimas no paguen.

Los afiliados no solo tienen control total sobre las negociaciones, sino que se quedan con el 80% de cada pago de rescate. Lynx incluso ofrece "servicios adicionales", como centros de llamadas para acosar a las víctimas y soluciones de almacenamiento avanzadas para sus miembros más exitosos.

Para garantizar que los archivos sean irrecuperables sin pagar el rescate, Lynx usa algoritmos de cifrado avanzados como Curve25519 Donna y AES-128.

Como muchas otras bandas de ransomware, Lynx emplea la doble extorsión:

- Primero cifran los archivos y exigen un rescate.
- Si la víctima no paga, publican los datos robados en su propio sitio de filtraciones (DLS).

Indicadores de Compromiso:

Ransomware Makop

- Ransomware Makop (mkp_visual.exe)
  -> MD5: 48b493c1e9795a8d28a511d88b86f9e
  -> SHA256: 4aace7fd7ba4c0eb24454f9bbf161499363ff34fc5c2eb81b982a25cfc0fdd27
- Ransomware Crysis (5-2NS.exe)
  -> MD5: 6bffc6c7caa2eb2fa90fac0317f63338
  -> SHA256: 92c65b58c4925534c2ce78e54b0e11ecaf45ed8cf0344ebff46cdfc4f2fe0d84
- Trojan.Win64.Occamy (LostMyPassword.exe)
  -> MD5: 5f3583d76b81f91d2f63813414cd5b47
  -> SHA256: 7da421d00cd50570a79a82803c170d043fa3b2253ae2f0697e103072c34d39f1
- arestore.exe -> 7f86b67ac003eda9d2929c9317025013
- data.exe -> e245f8d129e8eadb00e165c569a14b71
- Advanced_Port_Scanner_2.5.3869.exe -> 6A58B52B184715583CDA792B56A0A1ED
- Everything.exe -> b69d036d1dcfc5c0657f3a1748608148
- YDArk.exe -> 9fd28d2318f66e4fe37a9a5bc1637928

Ransomware Lynx

Hashes SHA256

- 571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b
- 82eb1910488657c78bef6879908526a2a2c6c31ab2f0517fcc5f3f6aa588b513
- eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc
- b378b7ef0f906358eec595777a50f9bb5cc7bb6635e0f031d65b818a26bdc4ee
- ecbfea3e7869166dd418f15387bc33ce46f2c72168f571071916b5054d7f6e49
- 85699c7180ad77f2ede0b15862bb7b51ad9df0478ed394866ac7fa9362bf5683

Correo electrónico del contacto de la nota sobre el ransomware Lynx

- martina.lestariid1898@proton[.]me

Blog de acceso público sobre la filtración del ransomware Lynx

- lynxblog[.]net

URL de Tor para el ransomware Lynx:

- hxxp[:]//lynxbllrfr5262yvbgtqoyq76s7mpztcqkv6tjjxgpilpma7nyoeohyd[.]onion
- hxxp[:]//lynxbllrfr5262yvbgtqoyq76s7mpztcqkv6tjjxgpilpma7nyoeohyd[.]onion/disclosures
- hxxp[:]//lynxblogco7r37jt7p5wrmfxzqze7ghxw6rihzkqc455qluacwotciyd[.]onion
- hxxp[:]//lynxblogijy4jfoblgix2klxmkbgee4leoeuge7qt4fpfkj4zbi2sjyd[.]onion
- hxxp[:]//lynxblogmx3rbiwg3rpj4nds25hjsnrwkpxt5gaznetfikz4gz2csyad[.]onion
- hxxp[:]//lynxblogoxllth4b46cfwlop5pfj4s7dyv37yuy7qn2ftan6gd72hsad[.]onion
- hxxp[:]//lynxblogtwatfsrwj3oatpejwxk5bngqcd5f7s26iskagfu7ouaomjad[.]onion
- hxxp[:]//lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd[.]onion

- hxxp[:]//lynxblogxutufossaeawlij3j3uikalolI5ko6grzhkwdclrjngrfoid[.]onion
- hxxp[:]//lynxch2k5xi35j7hlbmwl7d6u2oz4vp2wqp6qkwol624cod3d6iqiyqd[.]onion/login
- hxxp[:]//lynxchatbykq2vycvyrtjqb3yuj4ze2wvdubzr2u6b632trwvdbsgmyd[.]onion/login
- hxxp[:]//lynxchatde4spv5x6xlwxf47jdo7wtwwgikdoeroxamphu3e7xx5doqd[.]onion/login
- hxxp[:]//lynxchatdy3tgcuijsqofhssopcepirjfq2f4pvb5qd4un4dhqyxswqd[.]onion/login
- hxxp[:]//lynxchatdykpoelffqlvcbtry6o7gxk3rs2aiagh7ddz5yfttd6quxqd[.]onion/login
- hxxp[:]//lynxchatfw4rgsclp4567i4llkqjr2kltaumwwobxdik3qa2oorrknad[.]onion/login
- hxxp[:]//lynxchatly4zludmhmi75jrwhycnoqvkxb4prohxmyzf4euf5gjxroad[.]onion/login
- hxxp[:]//lynxchatohmppv6au67lloc2vs6chy7nya7dsu2hhs55mcjxp2joglad[.]onion/login

3. RECOMENDACIONES:

- Realizar el bloqueo de los indicadores de compromiso listados.
- Realizar auditorías de seguridad periódicas para detectar vulnerabilidades.
- Deshabilitar los puertos de acceso remoto/Protocolo de escritorio remoto (RDP) no utilizados y monitorear los registros de acceso/RDP.
- Programar copias de seguridad periódicas y automáticas de la información crítica y almacenarlas en ubicaciones seguras siguiendo la estrategia 3-2-1-1-0, que consiste en realizar periódicamente 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 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.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones de ransomware
- Habilitar la protección de red para evitar que las aplicaciones o los usuarios accedan a dominios maliciosos y otro contenido malicioso en Internet.
- Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados. Estos programas pueden detectar y eliminar ransomware y otro software malicioso antes de que puedan cifrar sus archivos.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://blog.ehcgroup.io/2025/01/29/14/28/44/18002/cuidado-ransomware-makop-y-lynx-activos-en-america-latina/seguridad-informatica/ransonware/ehacking/ • hxxps://blog.tecnetone.com/ransomware-makop-y-lynx-atacan-organizaciones-en-am%C3%A9rica-latina?hs_amp=true • hxxps://medium.com/@lcam/makop-the-toolkit-of-a-criminal-gang-53cd44563c11 • hxxps://unit42.paloaltonetworks.com/inc-ransomware-rebrand-to-lynx/

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°024	Fecha: 29-01-2025
		Página: 7 de 14

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Ciberdelincuentes aprovechan el Año Nuevo Chino para crear tiendas 'online' fraudulentas		
Tipo de Ataque	Portal fraudulento	Abreviatura	PortalFrau
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G02
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Expertos en ciberseguridad han advertido que durante los días previos al Año Nuevo Chino 2025, que se celebra este miércoles, se ha disparado el número de páginas web fraudulentas en las que se promueven regalos con descuentos cuyos pagos acaban en manos de los estafadores.

Este evento, celebrado en todo el mundo, así como su creciente popularidad lo convierte en un objetivo atractivo para los ciberdelincuentes, aprovechándose una vez más de las tendencias globales y del entusiasmo de los consumidores y el espíritu festivo

2. DETALLES:

Kaspersky indicó que, en la víspera de esta celebración, se crearon diversas tiendas online fraudulentas con el objetivo de atraer a posibles compradores con ofertas atractivas, creando un sentido de urgencia para realizar compras rápidamente.

Una vez que la víctima introduce sus datos bancarios y realiza el pago, los estafadores desaparecen y dejan a los consumidores globales sin su dinero y sus compras.

Además, se ha detectado que algunos de los ciberdelincuentes ni siquiera se molestan en actualizar los productos de sus tiendas en línea. Siguen mostrando artículos con el dragón, símbolo del año anterior.

3. RECOMENDACIONES:

- Verificar la autenticidad de las páginas web y revisar las URLs de cualquier tienda online, así como los nombres de dominio y las opiniones de otros clientes antes de realizar una compra
- Desconfiar de ofertas no solicitadas, pues los estafadores también pueden emplear ventanas emergentes, anuncios o correos electrónicos de "phishing" para llevar a los usuarios a sitios fraudulentos.
- No compartir información personal ni proporcionar datos sensibles a menos que se haya confirmado que se trata de plataformas seguras y verificadas.
- Implementar soluciones de ciberseguridad para prevenir infecciones de malware.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Cambiar las contraseñas predeterminadas a contraseñas seguras y cambiarlas periódicamente.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Implementar herramientas de monitoreo de red para identificar cualquier actividad sospechosa o intentos de acceso no autorizado.
- Educar a los empleados sobre las amenazas de correo electrónico malicioso o intentos de phishing, y cómo identificarlos.

Fuente de Información:	• hxxps://www.escudodigital.com/ciberseguridad/ano-nuevo-chino-gancho-ciberestafas-webs-fraudulentas_62079_102.html • hxxps://www.unotv.com/tecnologia/ano-nuevo-chino-2025-atacantes-crean-tiendas-online-fraudulentas/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°024	Fecha: 29-01-2025 Página: 8 de 14

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de escalada de privilegios en el complemento Post Grid y Gutenberg Blocks para WordPress		
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 gestión inadecuada de privilegios en el complemento Post Grid y Gutenberg Blocks de PickPlugins para WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado aumentar los privilegios y tomar de control total de los sitios afectados.

2. DETALLES:

La vulnerabilidad de severidad **ALTA** identificada por MITRE como CVE-2024-9636 de tipo gestión inadecuada de privilegios en el complemento Post Grid y Gutenberg Blocks para WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado aumentar los privilegios. Esta vulnerabilidad permite la escalada de privilegios, lo que significa que un atacante podría obtener mayores privilegios de los previstos dentro del sistema, lo que podría llevar a un acceso o control no autorizado sobre los sitios de WordPress afectados.

La vulnerabilidad existe debido a que el complemento afectado no restringe adecuadamente qué metadatos del usuario se pueden actualizar durante el registro del perfil. Un atacante remoto puede registrarse en el sitio como administrador.

A. Productos afectados:

- Post Grid y Gutenberg Blocks – ComboBlocks: 2.2.85 - 2.3.3.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://plugins.trac.wordpress.org/browser/post-grid/tags/2.2.93/includes/blocks/form-wrap/functions.php#L3200 • hxxp://plugins.trac.wordpress.org/changeset/3117675/post-grid/trunk/includes/blocks/form-wrap/functions.php • hxxp://plugins.trac.wordpress.org/changeset/3221012/post-grid/trunk/includes/blocks/form-wrap/functions.php • hxxp://www.wordfence.com/threat-intel/vulnerabilities/id/1bbe01b8-24ed-4e1e-bafc-0f4dea96c1f3?source=cve

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°024	Fecha: 29-01-2025 Página: 9 de 14

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades de severidad crítica en el dispositivo FactoryTalk 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 **CRÍTICA** de tipo inyección de comando del SO y autorización incorrecta que afecta a FactoryTalk View ME. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código en el dispositivo con privilegios elevados.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-24479 de tipo autorización incorrecta, podría permitir a un atacante remoto la ejecución de código local en los productos FactoryTalk de Rockwell Automation en todas las versiones anteriores a la versión 15.0. La vulnerabilidad se debe a una configuración predeterminada en Windows y permite el acceso al símbolo del sistema como un usuario con privilegios superiores.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-24480 de tipo inyección de comando del SO, podría permitir a un atacante remoto ejecución remota de código en los productos FactoryTalk de Rockwell Automation en todas las versiones anteriores a la versión 15.0. La vulnerabilidad se debe a la falta de limpieza de la entrada y podría permitir que un atacante remoto ejecute comandos o código como un usuario con privilegios elevados.

A. Productos afectados:

- FactoryTalk View ME: todas las versiones anteriores a la 15.0.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Minimizar la exposición de la red para todos los dispositivos y/o sistemas del sistema de control, garantizando que no sean accesibles desde Internet.
- Ubicar redes de sistemas de control y dispositivos remotos detrás de firewalls y aislarlos de las redes comerciales.
- Utilizar métodos más seguros, como redes privadas virtuales (VPN), teniendo en cuenta que las VPN pueden tener vulnerabilidades y deben actualizarse a la versión más reciente disponible. Además, tener en cuenta que la seguridad de una VPN depende de los dispositivos conectados

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-028-03 • hxxps://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1085012/loc/en_US#__highlight

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°024	Fecha: 29-01-2025 Página: 10 de 14

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en VMware Avi Load Balancer		
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:

Broadcom Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo inyección SQL ciega no autenticada en VMware Avi Load Balancer. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener acceso no autorizado a datos confidenciales almacenados en la base de datos, lo que provocaría violaciones de datos que comprometerían la información confidencial de los usuarios y de la organización.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-22217 de tipo inyección SQL ciega no autenticada en VMware Avi Load Balancer, podría permitir a un atacante remoto no autenticado obtener acceso no autorizado a datos confidenciales.

La vulnerabilidad se origina en una limpieza inadecuada de las entradas, lo que permite a los atacantes utilizar consultas SQL especialmente diseñadas para obtener acceso a la base de datos. Esto significa que un actor malintencionado podría manipular las consultas de la base de datos para extraer información confidencial, modificar datos o incluso tomar el control de todo el sistema.

Las organizaciones que utilizan versiones afectadas de VMware Avi Load Balancer deben priorizar la actualización de sus sistemas para protegerse contra esta grave falla de seguridad.

A. Productos afectados:

- VMware Avi Load Balancer, versión 30.1.1, 30.1.2, 30.2.1 y 30.2.2.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad. VMware confirma que no existen soluciones alternativas para este problema, por lo que la aplicación de parches es la única estrategia de mitigación eficaz.

Fuente de Información:	• hxxps://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25346

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°024	Fecha: 29-01-2025
		Página: 11 de 14

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en TeamViewer para Windows		
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 inyección de argumentos que afecta a los clientes de TeamViewer para Windows. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado escalar privilegios locales en un sistema Windows.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-0065 de tipo inyección de argumentos que afecta a los clientes de TeamViewer para Windows, podría permitir a un atacante remoto no autenticado escalar privilegios locales en un sistema Windows.

La neutralización incorrecta de los delimitadores de argumentos en el componente TeamViewer_service.exe de TeamViewer Full Client & Host anterior a la versión 15.62 (y las versiones adicionales enumeradas a continuación) para Windows permite a un atacante con acceso local sin privilegios en un sistema Windows elevar los privilegios mediante la inyección de argumentos. Para aprovechar esta vulnerabilidad, un atacante necesita acceso local al sistema Windows.

TeamViewer AG indico que no tiene a la fecha indicios de que esta vulnerabilidad haya sido o esté siendo explotada en la naturaleza.

A. Productos afectados:

- TeamViewer: 11.0.214397 - 15.61.4.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.teamviewer.com/en/resources/trust-center/security-bulletins/tv-2025-1001/?

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°024	Fecha: 29-01-2025 Página: 12 de 14

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Schneider Electric		
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:

Schneider Electric SE ha publicado una vulnerabilidad de severidad **ALTA** de tipo deserialización de datos que no son de confianza que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante la ejecución remota de código en estaciones de trabajo cuando un usuario autenticado que no sea administrador abra un archivo de proyecto malicioso.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-12703 de tipo deserialización de datos que no son de confianza que afectan a múltiples productos de Schneider Electric, podría permitir a un usuario autenticado que no es administrador abrir un archivo de proyecto.

Los atacantes pueden explotar esta vulnerabilidad de forma local sin necesidad de autenticación. Para ello, es necesaria la interacción del usuario, como abrir un archivo malicioso.

Existe una vulnerabilidad de deserialización de datos no confiables que podría provocar pérdida de confidencialidad, integridad y posible ejecución remota de código en la estación de trabajo cuando un usuario autenticado que no es administrador abre un archivo de proyecto malicioso.

A. Productos afectados:

- Electric RemoteConnect, todas las versiones.
- SCADAPackTM x70 Utilities, todas las versiones.

3. RECOMENDACIONES:

- Estar atentos a las publicaciones de Schneider Electric sobre la elaboración de un plan de reparación para todas las versiones futuras de RemoteConnect y SCADAPackTM x70 Utilities, la cual incluirá una solución para esta vulnerabilidad.
- Abrir únicamente archivos de proyecto recibidos de una fuente confiable.
- Calcular un hash de los archivos del proyecto y verifique periódicamente la consistencia de este hash para verificar la integridad antes de su uso.
- Cifrar el archivo del proyecto cuando se almacena y restringir el acceso solo a usuarios confiables.
- Utilizar protocolos de comunicación seguros al intercambiar archivos a través de la red.
- Seguir las pautas de seguridad de SCADAPackTM.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-028-06 • hxxps://www.se.com/ww/en/download/document/SCADAPack_Cybersecurity_Guide/ • hxxps://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-014-06&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-014-06.pdf

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°024	Fecha: 29-01-2025 Página: 13 de 14

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en dispositivos Moxa		
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:

Moxa Technologies ha publicado una vulnerabilidad de severidad **ALTA** de tipo escritura fuera de límites que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado generar una condición de denegación de servicio (DoS).

2. DETALLES:

Moxa Technologies es una empresa tecnológica especializada en soluciones de conectividad periférica, informática industrial e infraestructura de red.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-7695 de tipo escritura fuera de límites en varios productos MOXA, podría permitir a un atacante remoto no autenticado generar una condición de DoS.

La vulnerabilidad de escritura fuera de límites causada por una validación de entrada insuficiente permite a los atacantes sobrescribir la memoria más allá de los límites del búfer. La explotación exitosa de esta vulnerabilidad podría provocar una condición de DoS, lo que interrumpiría las operaciones normales.

A. Productos afectados:

- Serie PT-7728 Versión de firmware 3.9 y anteriores.
- Serie PT-7828 Versión de firmware 4.0 y anteriores.
- Serie PT-G503 Versión de firmware 5.3 y anteriores.
- Serie PT-G510 Versión de firmware 6.5 y anteriores.
- Serie PT-G7728 Versión de firmware 6.4 y anteriores.
- Serie PT-G7828 Versión de firmware 6.4 y anteriores.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Deshabilitar el servicio Moxa (cifrado) temporalmente si no son necesarios para las operaciones.

Fuente de Información:	• hxxps://www.moxa.com/en/support/product-support/security-advisory/mpsa-240162-cve-2024-7695-out-of-bounds-write-vulnerability-identified-in-multiple-pt-switches

Índice alfabético