



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

061-2026-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

CVE-2026-31431: 732 bytes para obtener privilegios de root en (casi) todos los servidores Linux.	4
Vect 2.0: Análisis técnico de operación ransomware y actividad en la Dark Web con enfoque en riesgos y mitigación.	6
Vulnerabilidades críticas en productos Cisco.	9
Índice alfabético	10

 Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°061		Fecha: 29-04-2026
			Página: 4 de 10
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	CVE-2026-31431: 732 bytes para obtener privilegios de root en (casi) todos los servidores Linux.		
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:

El 29 de abril de 2026 se hizo pública la vulnerabilidad crítica CVE-2026-31431, conocida como Copy Fail, tras ser divulgada por un investigador de Theori.io. Esta falla afecta al kernel de Linux y ha estado presente de forma silenciosa desde 2017, impactando prácticamente a todas las distribuciones modernas basadas en kernels 4.13 o superiores, como Ubuntu, RHEL, SUSE y Amazon Linux. La vulnerabilidad permite que un usuario sin privilegios elevados obtenga acceso root, lo que representa un riesgo severo para servidores, entornos cloud y plataformas Kubernetes, donde la confianza en los límites de privilegios es fundamental.



Ilustración 1 CVE-2026-31431: 732 bytes para obtener privilegios de root en (casi) todos los servidores Linux.

2. DETALLES:

Copy Fail permite que un atacante logre una escalada de privilegios utilizando un script en Python extremadamente pequeño, de apenas 732 bytes, sin necesidad de técnicas avanzadas ni condiciones de carrera específicas. El exploit se aprovecha de un fallo en la gestión de la page cache del kernel de Linux, alterando únicamente la versión en memoria de binarios sensibles como /usr/bin/su, mientras el archivo original en disco permanece intacto. Debido a esto, los mecanismos tradicionales de control de integridad basados en hashes de archivos no identifican ningún cambio malicioso.

La característica compartida de la page cache entre procesos hace que esta vulnerabilidad tenga un alcance especialmente crítico en entornos contenerizados. Un compromiso inicial dentro de un contenedor o pod puede escalar hasta el nodo Kubernetes subyacente, afectando a todas las cargas de trabajo que se ejecutan en él. El impacto es transversal y alcanza tanto infraestructuras on-premise como entornos cloud, posicionando a esta CVE como una de las fallas más graves en la historia reciente del kernel Linux.

3. RECOMENDACIONES:

- Actualizar inmediatamente el kernel de Linux a una versión que incluya el parche (corrección integrada al mainline el 1 de abril de 2026) y reiniciar los sistemas afectados.
- Inventariar versiones de kernel en todos los servidores, VMs y nodos Kubernetes para identificar exposición real.
- Aplicar mitigaciones temporales, como deshabilitar el módulo vulnerable del kernel o restringir la syscall afectada mediante perfiles seccomp en contenedores, mientras se despliegan los parches definitivos.
- Planificar reinicios controlados (drain & cordon en Kubernetes) para evitar indisponibilidad en producción.
- Fortalecer monitoreo de comportamiento, incorporando detección en memoria y análisis de llamadas al sistema, no solo controles basados en archivos.
- Reducir privilegios y superficie de ataque, limitando accesos de usuarios locales y endureciendo la configuración del sistema operativo base.
- Integrar gestión de parches al ciclo de seguridad, considerando al kernel como un componente crítico y no solo al software de aplicación.

Fuente de Información:

- <https://www.loginline.com/en/blog/cve-2026-31431>

	ALERTA DE SEGURIDAD DIGITAL N°235		Fecha: 29-04-2026
			Página: 6 de 10
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vect 2.0: Análisis técnico de operación ransomware y actividad en la Dark Web con enfoque en riesgos y mitigación.		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C09
Clasificación temática familia	Código malicioso		

Descripción

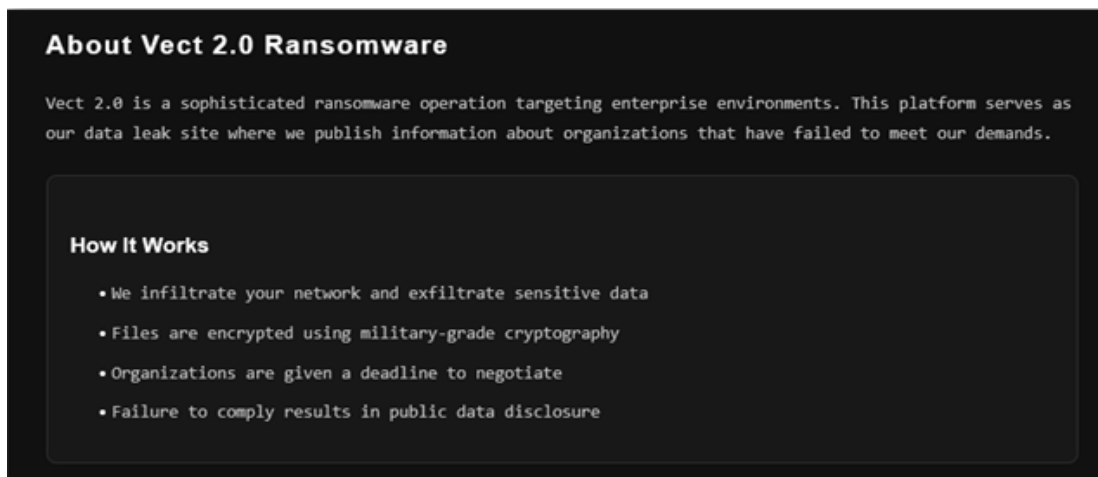
1. ANTECEDENTES:

El informe identifica a Vect 2.0 como una operación emergente de Ransomware-as-a-Service (RaaS) que experimentó un incremento significativo de actividad durante febrero de 2026. Este grupo, activo desde diciembre de 2025, ha evolucionado rápidamente posicionándose dentro del ecosistema criminal mediante un modelo de negocio claramente definido basado en “Exfiltration / Encryption / Extortion” (triple extorsión). A nivel operativo, su panel de filtración (Data Leak Site - DLS) registró 20 víctimas activas, de las cuales 6 ya tenían datos publicados y 14 se encontraban en proceso de negociación o extorsión, evidenciando una campaña activa y sostenida.

Los sectores más afectados por el grupo de ransomware Vect 2.0 son la industria manufacturera, la educación, la sanidad y la tecnología.

2. DETALLES:

Desde una perspectiva de actividad en la dark web, Vect 2.0 demuestra un alto grado de madurez operativa. Toda su infraestructura —incluyendo el DLS, portales de negociación y canales de comunicación— opera exclusivamente sobre la red TOR, eliminando exposición en la clearnet y dificultando la atribución. Además, el grupo utiliza el protocolo TOX para comunicaciones cifradas peer-to-peer y exige pagos exclusivamente en Monero (XMR), lo que refuerza el anonimato financiero. El modelo de afiliación incluye reclutamiento activo en foros clandestinos, con incentivos dirigidos a actores de países de la Comunidad de Estados Independientes (CIS), lo que sugiere un posible origen o núcleo operativo en regiones como Rusia o Bielorrusia.



El análisis de la actividad criminal revela que el ransomware Vect 2.0 no solo opera como un grupo aislado, sino como parte de un ecosistema ransomware altamente estructurado, donde la dark web funciona como plataforma de reclutamiento, negociación, publicación de filtraciones y reputación criminal. Su Data Leak Site actúa como mecanismo de presión psicológica y reputacional sobre las víctimas, reforzado por políticas de archivo que mantienen los datos expuestos durante meses. Este enfoque, combinado con una media de 8 días entre intrusión y publicación, demuestra una capacidad operativa ágil orientada a maximizar la extorsión en ventanas de tiempo reducidas.

La operación de Vect 2.0 se enmarca dentro de un modelo RaaS altamente estructurado, donde existe una clara separación entre desarrolladores y afiliados. Los desarrolladores mantienen el código del ransomware, la infraestructura en la red TOR y los portales de filtración, mientras que los afiliados ejecutan las intrusiones. Este modelo permite escalar rápidamente las operaciones y diversificar vectores de ataque. La evidencia del informe indica que el grupo utiliza un

esquema de triple extorsión, combinando cifrado de sistemas, exfiltración de datos y presión mediante publicación en su Data Leak Site (DLS), lo que incrementa significativamente la probabilidad de pago por parte de las víctimas.

En la fase de acceso inicial, la operación se apoya en la explotación de servicios expuestos a internet y el uso de credenciales comprometidas, lo que sugiere una fuerte dependencia de accesos válidos y vulnerabilidades en aplicaciones públicas. Este enfoque reduce la necesidad de campañas masivas de phishing y permite ataques más dirigidos. El uso de inteligencia obtenida en la dark web facilita la selección de objetivos con alta probabilidad de compromiso. Aunque el informe no detalla vectores específicos, este patrón es consistente con técnicas como explotación de aplicaciones web y acceso mediante cuentas válidas.

Una vez dentro del entorno, los afiliados despliegan cargas maliciosas diseñadas para persistencia y ejecución evasiva. El ransomware Vect 2.0, desarrollado en C++, presenta capacidades multiplataforma (Windows, Linux y entornos virtualizados como ESXi), lo que amplía su impacto en infraestructuras empresariales. La ejecución en Safe Mode observada en este tipo de amenazas permite evadir soluciones EDR y antivirus, mientras que el uso de cifrado optimizado acelera el proceso de impacto. Adicionalmente, el comportamiento reportado sugiere que en algunos casos puede actuar como wiper, destruyendo datos irreversiblemente, lo que incrementa el riesgo operativo.

Durante la fase de movimiento lateral y escalada de privilegios, los atacantes realizan reconocimiento interno y reutilización de credenciales para expandirse dentro de la red comprometida. La falta de segmentación de red y controles de acceso robustos facilita el compromiso de sistemas críticos, incluidos servidores y plataformas de virtualización. Este comportamiento es consistente con campañas modernas de ransomware que priorizan la toma de control de activos de alto valor antes de ejecutar el cifrado.

En la etapa final, la operación establece canales de comando y control (C2) a través de infraestructura anónima en TOR, utilizando protocolos cifrados y herramientas como TOX para la comunicación directa con las víctimas. La exfiltración de datos se realiza antes del cifrado, permitiendo al grupo ejercer presión adicional mediante amenazas de publicación. El uso exclusivo de Monero (XMR) para pagos refuerza el anonimato financiero y dificulta el rastreo de transacciones. La rapidez operativa —con ventanas de aproximadamente 8 días entre intrusión y publicación— evidencia un proceso altamente optimizado orientado a maximizar beneficios.

Vect 2.0 evidencia la evolución del ransomware hacia modelos operativos altamente industrializados, donde la combinación de anonimato, automatización y monetización eficiente incrementa significativamente el riesgo para organizaciones públicas y privadas. La ausencia de CVEs específicos en el informe refuerza la hipótesis de que el éxito de estas campañas no depende de vulnerabilidades aisladas, sino de la explotación sistemática de debilidades estructurales: exposición de servicios, gestión deficiente de identidades y falta de segmentación. En este contexto, la defensa efectiva requiere un enfoque integral basado en reducción de superficie de ataque, detección temprana y resiliencia operativa.

A. Vulnerabilidades explotadas:

- El informe oficial no proporciona identificadores CVE específicos asociados a la operación de Vect 2.0,
- No obstante, el patrón técnico descrito indica explotación probable de:
 - Aplicaciones web expuestas sin parchear,
 - Servicios remotos con autenticación débil,
 - Infraestructura virtualizada mal configurada (ej. ESXi).

B. Indicadores de Compromiso (IoC):

- IP: 158.94.210.11:8000,
- Archivos maliciosos: svc_host_update.exe, enc_esxi.elf,
- Notas de rescate: VECT_RECOVERY_GUIDE.txt, README_VECT.html,
- Correo asociado: Qilin[@]exploit[.]im,
- Extensión: .vect.

C. Datos clave del incidente:

- Tipo: Ransomware (RaaS) con triple extorsión,
- Madurez: Media-alta (en rápida evolución),
- Capacidades clave: Infraestructura anónima robusta, Monetización eficiente, Reclutamiento activo,

- Participación en el ecosistema: ~1.6% de incidentes observados (febrero 2026).

3. RECOMENDACIONES:

Superficie de ataque y acceso inicial:

- Aplicar gestión continua de vulnerabilidades con priorización basada en criticidad,
- Reducir la exposición de servicios a internet (principio de mínimo acceso),
- Implementar autenticación multifactor (MFA) en accesos remotos y administrativos,
- Monitorear credenciales filtradas en fuentes de inteligencia de amenazas,

Detección y respuesta:

- Implementar soluciones EDR/XDR con capacidades de detección basada en comportamiento,
- Supervisar ejecución en Safe Mode y eventos anómalos del sistema,
- Correlacionar eventos de autenticación sospechosos (uso de cuentas válidas fuera de patrón),

Segmentación y contención:

- Segmentar redes críticas para limitar movimiento lateral,
- Aplicar principios de Zero Trust en accesos internos,
- Restringir privilegios administrativos y aplicar control de cuentas privilegiadas (PAM),

Protección de datos:


- Implementar estrategias de backup offline e inmutables,
- Validar periódicamente la recuperación de datos,
- Monitorear actividades de exfiltración de datos,

Preparación y resiliencia:

- Realizar ejercicios de respuesta a incidentes (IR) enfocados en ransomware,
- Integrar inteligencia de amenazas en operaciones SOC,
- Establecer playbooks específicos para eventos de doble/triple extorsión.

Fuente de Información:

- <https://securityaffairs.com/191374/security/firefox-bug-cve-2026-6770-enabled-cross-site-tracking-and-tor-fingerprinting.html>
- <https://www.sentinelone.com/vulnerability-database/cve-2026-6770/>
- <https://www.tenable.com/cve/CVE-2026-6770>
- <https://www.rapid7.com/db/vulnerabilities/mfsa2026-30-cve-2026-6770/>

	ALERTA DE SEGURIDAD DIGITAL N°236		Fecha: 29-04-2026
			Página: 9 de 10
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades críticas en productos Cisco.		
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>Cisco Systems, Inc. ha publicado dos vulnerabilidades de severidad CRÍTICA clasificadas como CWE-22: Limitación indebida de una ruta de acceso a un directorio restringido (recorrido de ruta) y CWE-77: Neutralización incorrecta de elementos especiales utilizados en un comando (Inyección de comandos) que afecta a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto autenticado ejecute código de forma remota o realice ataques de recorrido de ruta en un dispositivo afectado. Para explotar estas vulnerabilidades, el atacante debe contar con credenciales administrativas válidas.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad crítica identificada por MITRE como CVE-2026-20147 clasificada como CWE-77: Inyección de comandos en Cisco ISE y Cisco ISE-PIC, podría permitir que un atacante remoto autenticado ejecute comandos arbitrarios en el sistema operativo subyacente de un dispositivo afectado. Para explotar esta vulnerabilidad, el atacante debe contar con credenciales administrativas válidas. Esta vulnerabilidad se debe a una validación insuficiente de la información proporcionada por el usuario. Un atacante podría explotarla enviando una solicitud HTTP manipulada a un dispositivo afectado. Una explotación exitosa podría permitir al atacante obtener acceso de nivel de usuario al sistema operativo subyacente y, posteriormente, elevar sus privilegios a root. En implementaciones de ISE de nodo único, la explotación exitosa de esta vulnerabilidad podría provocar que el nodo ISE afectado quede inaccesible, lo que resultaría en una denegación de servicio (DoS). En tal caso, los puntos finales que no se hayan autenticado previamente no podrían acceder a la red hasta que se restablezca el nodo.</p> <p>La vulnerabilidad de severidad media identificada por MITRE como CVE-2026-20148 clasificada como CWE-22: Recorrido de ruta en Cisco ISE y Cisco ISE-PIC, podría permitir que un atacante remoto autenticado realice ataques de recorrido de ruta en el sistema operativo subyacente y lea archivos arbitrarios. Para explotar esta vulnerabilidad, el atacante debe tener credenciales administrativas válidas. Esta vulnerabilidad se debe a una validación incorrecta de los datos introducidos por el usuario. Un atacante podría explotarla enviando una solicitud HTTP manipulada al sistema afectado. Si la explotación es exitosa, el atacante podría acceder a archivos confidenciales en dicho sistema.</p> <p>Las vulnerabilidades no son interdependientes. La explotación de una vulnerabilidad no es necesaria para explotar otra. Además, una versión de software afectada por una vulnerabilidad puede no verse afectada por las demás.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> Estas vulnerabilidades afectan a Cisco ISE y Cisco ISE-PIC, independientemente de la configuración del dispositivo. Cisco ISE-PIC ha llegado al final de su ciclo de ventas. La versión 3.4 es la última versión compatible. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> Cisco ha publicado actualizaciones de software que solucionan estas vulnerabilidades. No existen soluciones alternativas para corregirlas. 			
Fuente de Información:	<ul style="list-style-type: none"> hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-traversal-8bYndVrZ 		

Índice alfabético

Ransomware	6
Explotación de vulnerabilidades conocidas	4,9