



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

137-2025-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 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

DragonForce explota SimpleHelp sin parche para implantar ransomware en clientes de un MSP

4

Vulnerabilidades de severidad crítica en VMware Salt

6

Vulnerabilidad de uso posterior a la liberación en Adobe Acrobat y Adobe Reader

7

Índice alfabético

8

 Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 137		Fecha: 13-06-2025
			Página: 4 de 8
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	DragonForce explota SimpleHelp sin parche para implantar ransomware en clientes de un MSP		
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:			
Investigadores de Sophos han documentado una campaña en la que el grupo DragonForce comprometió un Managed Service Provider (MSP) aprovechando tres fallos críticos en el software RMM SimpleHelp. El ransomware DragonForce es una marca avanzada y competitiva de ransomware como servicio (RaaS) que apareció por primera vez a mediados de 2023. Como se analiza en una investigación reciente de Sophos Counter Threat Unit (CTU), DragonForce comenzó en marzo a esforzarse por cambiar su imagen de marca para convertirse en un “cártel” y pasar a un modelo de marca afiliada distribuida. SimpleHelp es una herramienta de soporte al cliente y acceso remoto que se utiliza en diversos escenarios comerciales; sin embargo, como muchas otras herramientas de acceso remoto, también es un objetivo popular para los actores de amenazas que buscan obtener acceso de alto nivel ya sea a través de vulnerabilidades (como en este caso) o estafas de soporte técnico/ataques de ingeniería social.			
2. DETALLES:			
Los criminales encadenan las siguientes vulnerabilidades divulgadas en enero de 2025: – 2024-57727 - Recorrido de ruta -> Descarga de archivos de configuración con hashes y secretos. – 2024-57726 - Escalada de privilegios -> De técnico con pocos permisos a admin completo. – 2024-57728 - Carga arbitraria de ficheros -> Ejecución remota de código en el servidor. Una vez dentro, los operadores empujan instaladores maliciosos a los endpoints gestionados, realizan reconocimiento (usuarios, red, configuraciones) y despliegan DragonForce con táctica de doble extorsión. Todas las instalaciones SimpleHelp igual o menores a 5.5.7 (Windows, Linux y macOS) son vulnerables. El proveedor publicó la versión 5.5.8 en enero, pero muchos MSP siguen sin aplicar el parche. Impacto potencial – Compromiso completo del servidor RMM y de todos los clientes gestionados. – Implantación de ransomware y robo de datos para extorsión múltiple. – Elevados costes operativos y reputacionales para el MSP y sus clientes finales. Además de enviar maliciosamente la instancia de SimpleHelp a los clientes, el atacante usó el acceso al MSP para acceder a muchos de sus clientes. Uno de los clientes del MSP logró bloquear el acceso del atacante a la red mediante MDR y capacidades de detección y respuesta extendidas (XDR), pero otros clientes posteriores se vieron afectados por ransomware y robo de datos, lo que dio lugar a ataques de doble extorsión. El portavoz de SimpleHelp indicó: "La mayoría de nuestros clientes actualizan su sistema poco después de publicar una nueva versión, o en este caso, lo hicieron tras nuestros boletines de seguridad. Hasta donde sabemos, ninguno de los que actualizaron a una versión segura (ni aplicaron los parches gratuitos que pusimos a disposición de los usuarios en versiones anteriores) en los días posteriores se ha visto afectado por la explotación de estas vulnerabilidades. Lamentablemente, los CVE y los detalles de la vulnerabilidad se hicieron públicos poco después, antes de que algunos de nuestros clientes actualizaran".			

3. RECOMENDACIONES:

- Actualizar inmediatamente a 5.5.8 o posterior.
- Restringir el acceso a la consola RMM por IP/VPN y deshabilitar la exposición pública del endpoint para todas las versiones.
- Revisar logs en busca de descargas sospechosas de serverconfig.xml y de instaladores SimpleHelp no autorizados.
- Monitorear el tráfico entrante y saliente inusual desde el servidor SimpleHelp (para clientes posteriores).
- Aplicar EDR/XDR en los clientes para detectar ejecución anómala de scripts o binarios con nombres aleatorios de tres letras.
- Cambiar todas las credenciales de técnicos y aplicar MFA en la administración de SimpleHelp.
- Aplicar protocolos estrictos de verificación de identidad para las interacciones de TI y de soporte técnico.
- Realizar ejercicios de mesa de trabajo con regularidad.
- Notificar a los clientes posteriores e indicarles que tomen medidas para proteger sus puntos finales
- Mantener copias de seguridad periódicas, limpias y sin conexión
- Abstenerse de exponer servicios remotos como el Protocolo de Escritorio Remoto (RDP) en la web.



Fuente de Información:

- <https://thehackernews.com/2025/06/ransomware-gangs-exploit-unpatched.html>
- <https://unaaldia.hispasec.com/2025/06/dragonforce-explota-simplehelp-sin-parche-para-implantar-ransomware-en-clientes-de-un-msp.html>
- <https://www.darkreading.com/application-security/dragonforce-ransomware-msp-supply-chain-attack>
- <https://news.sophos.com/es-es/2025/06/04/los-actores-de-dragonforce-aprovechan-las-vulnerabilidades-de-simplehelp-para-atacar-a-un-msp-y-a-sus-clientes/>

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 137		Fecha: 13-06-2025
			Página: 6 de 8
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades de severidad crítica en VMware Salt		
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 CRÍTICA de tipo recorrido de ruta que afecta a VMware Salt, específicamente a la clase VirtKey. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante local autenticado sobrescribir archivos en el sistema, lo que podría provocar una escalada de privilegios u otros resultados maliciosos.			
2. DETALLES:			
VMware ha integrado SaltStack (ahora conocido como Salt), especialmente en soluciones como vRealize Automation, para ofrecer automatización y gestión de infraestructura tanto física como virtual. Salt permite gestionar máquinas virtuales (VMs) y otros recursos a través de módulos específicos y el modelo maestro-minion, facilitando tareas como el aprovisionamiento, configuración y orquestación de VMs. La vulnerabilidad de severidad crítica identificada por MITRE como CVE-2025-22241 de tipo recorrido de ruta en la clase VirtKey del proyecto Salt ocurre cuando se solicitan datos del pilar bajo demanda y utiliza datos no validados para crear rutas al directorio PKI. Esta función se utiliza para aceptar automáticamente las claves de autenticación de Minion basándose en un archivo de autorización preinstalado en una ubicación específica y está presente en la configuración predeterminada. Un atacante con privilegios elevados podría explotar esta vulnerabilidad para sobrescribir el contenido de los archivos en el directorio PKI. Esto podría provocar la modificación no autorizada de las claves de autenticación, lo que podría comprometer la integridad de la infraestructura de Salt y permitir el acceso no autorizado o la omisión de la autenticación.			
A. Productos afectados:			
– Clase VirtKey en VMware Salt 3006.x < 3006.12 y 3007.x < 3007.4.			
3. RECOMENDACIONES:			
- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad. - Actualizar Salt a la versión 3006.12 o 3007.4 o posterior. - Restringir el acceso a los sistemas Salt para usuarios privilegiados. - Implementar una validación de entrada estricta para los datos de pilares. - Revisar y auditar las configuraciones del directorio PKI. - Supervisar cualquier modificación no autorizada a las claves de autenticación.			
Fuente de Información:		https://docs.saltproject.io/es/3006/topics/releases/3006.12.html https://docs.saltproject.io/es/3007/topics/releases/3007.4.html	

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 137		Fecha: 13-06-2025
			Página: 7 de 8
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de uso posterior a la liberación en Adobe Acrobat y Adobe Reader		
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:			
Adobe Systems Incorporated ha publicado una vulnerabilidad de severidad ALTA de tipo uso posterior a la liberación en Adobe Acrobat y Adobe Reader. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el contexto del usuario actual.			
2. DETALLES:			
La vulnerabilidad de severidad alta identificada por MITRE como CVE-2025-43574 de tipo uso posterior a la liberación en Adobe Acrobat y Adobe Reader, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y comprometer el sistema vulnerable.			
La vulnerabilidad existe debido a un error de uso tras liberación al gestionar archivos PDF. Un atacante remoto puede engañar a la víctima para que abra un archivo PDF especialmente diseñado y ejecute código arbitrario en el sistema. La explotación exitosa de la vulnerabilidad podría permitir a un atacante comprometer el sistema vulnerable.			
A. Productos afectados:			
– Adobe Acrobat: versiones anteriores a 20.005.30774, 24.001.30254, 25.001.20529, 25.001.20531.			
– Adobe Reader: versiones anteriores a 20.005.30774, 25.001.20529, 25.001.20531.			
3. RECOMENDACIÓN:			
• Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad.			
Fuente de Información:		• https://helpx.adobe.com/security/products/acrobat/apsb25-57.html • https://www.zerodayinitiative.com/advisories/ZDI-25-338/	

Índice alfabético

Explotación de vulnerabilidades conocidas	6, 7
Ransomware	4