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

172-2024-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

Nueva variante de Ransomware Play Apunta a Máquinas Virtuales VMware ESXi 4
Múltiples vulnerabilidades en los productos SICAM de Siemens 6
Vulnerabilidad crítica en Docker 7
Vulnerabilidad crítica en Spring Cloud Data Flow 8
Índice alfabético 9

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°172	Fecha: 25-07-2024
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Nueva variante de Ransomware Play Apunta a Máquinas Virtuales VMware ESXi		
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:

Se ha identificado una nueva variante en Linux del ransomware Play, que ataca entornos VMware ESXi. Este descubrimiento sugiere que el grupo detrás del ransomware Play podría estar ampliando sus ataques a la plataforma Linux, lo que daría lugar a un mayor número de víctimas y a negociaciones de rescate más exitosas.

Play ransomware apareció en junio de 2022 y sus operadores son conocidos por robar documentos sensibles de dispositivos comprometidos, utilizando estos datos en ataques de doble extorsión para presionar a las víctimas a pagar el rescate bajo la amenaza de filtrar los datos robados en línea.

Entre las víctimas del alto perfil de Play ransomware se encuentran la empresa de computación en la nube Rackspace, la ciudad de Oakland en California, el gigante minorista de automóviles Arnold Clark, la ciudad belga de Amberes y el condado de Dallas.

2. DETALLES:

Trend Micro, cuyos analistas detectan esta nueva variante de ransomware, explica que el locker está diseñado para verificar si se está ejecutando en un entorno ESXi antes de proceder con el cifrado. Además, tiene la capacidad de evadir la detección en sistemas Linux. Esta táctica resalta un movimiento estratégico de Play ransomware hacia un enfoque más amplio en sus ataques, lo que podría aumentar la cantidad de víctimas y la efectividad de las negociaciones de rescate.

Este cambio de enfoque no es nuevo. Durante años, la mayoría de los grupos de ransomware han dirigido sus ataques hacia las máquinas virtuales ESXi debido a que muchas empresas las utilizan para el almacenamiento de datos y la ejecución de aplicaciones críticas, gracias a su manejo más eficiente de los recursos.

Al analizar esta muestra de ransomware Play, Trend Micro descubrió que la pandilla utiliza los servicios de acortamiento de enlaces ilícitos proporcionados por un actor de amenazas conocido como Prolific Puma, para ayudarlos a evadir la detección mientras distribuyen malware.

Específicamente, emplea lo que se llama un algoritmo de generación de dominios registrados (RDGA) para generar nuevos nombres de dominio, un mecanismo programático que está siendo utilizado cada vez más por varios actores de amenazas, incluidos VexTrio Viper y Revolver Rabbit, para la propagación del spam de phishing y el malware.

Las muestras de ransomware Linux de Play escanearán y apagarán todas las VM en el entorno comprometido antes de comenzar a cifrar archivos (por ejemplo, archivos de disco de VM, configuración y metadatos), agregando la extensión .PLAY al final. de cada archivo.

Para apagar todas las máquinas virtuales VMware ESXi en ejecución y poder cifrarlas, el cifrador ejecutará el siguiente código:

```
/bin/sh -c "for vmid in $(vim-cmd vmsvc/getallvms | grep -v Vmid | awk '{print $1}'); do vim-cmd vmsvc/power.off $vmid; done"
```

Esta variante está diseñada específicamente para apuntar al sistema de archivos de máquinas virtuales (VMFS) utilizado por la suite de virtualización de servidores vSphere de VMware. También dejará una nota de rescate en el directorio raíz de la VM, que se mostrará en el portal de inicio de sesión del cliente ESXi y en la consola después de reiniciar la VM.

La interrupción de las máquinas virtuales ESXi de una organización puede provocar graves interrupciones y fallos en las operaciones comerciales. El cifrado de archivos y falta de copias de seguridad reduce las opciones de las víctimas para recuperar los datos afectados, aumentando así la presión para pagar el rescate.

3. RECOMENDACIONES:

- Deshabilitar los puertos de acceso remoto/Protocolo de escritorio remoto (RDP) no utilizados y monitorear los registros de acceso/RDP.
- Ejecutar la estrategia 3-2-1-1-0 de copias de seguridad, 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.
- 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.
- 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 y otro contenido maliciosos en Internet.
- Habilite la protección de firewall para monitorear y controlar el tráfico de red entrante y saliente.
- Implementar soluciones de seguridad avanzadas, como sistemas de detección y respuesta de endpoints (EDR), y software de detección y prevención de intrusiones (IDS/IPS), para identificar y bloquear comportamientos sospechosos antes de que causen daños significativos.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.
- En caso de infección, no pagar el rescate ni contactar con los ciberdelincuentes, ya que no hay garantía de que cumplan sus promesas. En su lugar, buscar ayuda profesional para eliminar el ransomware y restaurar los archivos cifrados. Así como también reportar el ransomware a las autoridades.

Fuente de Información:	• hxxps://devel.group/blog/nueva-variante-de-ransomware-play-apunta-a-maquinas-virtuales-vmware-esxi/ • hxxps://ciberplaneta.xyz/articles/22/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°172	Fecha: 25-07-2024
		Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en los productos SICAM de Siemens		
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 reportado dos vulnerabilidades de severidad **ALTA** de tipo cambio de contraseña no verificada y autenticación faltante para función crítica que afecta a varios productos SICAM de Siemens. La explotación exitosa de estas vulnerabilidades podría provocar una escalada de privilegios y una posible fuga de información. Un atacante remoto podría comprometer el sistema objetivo.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-37998 de tipo cambio de contraseña no verificada, podría permitir a un atacante remoto comprometer el sistema objetivo. La vulnerabilidad existe debido a la falta de validación adecuada de la contraseña anterior antes de establecer una nueva. Un atacante remoto puede obtener acceso administrativo a las aplicaciones de destino.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-39601 de tipo autenticación faltante para función crítica, podría permitir a un atacante remoto comprometer el sistema objetivo. La vulnerabilidad existe debido a la falta de autenticación para una función crítica. Un usuario remoto puede degradar el firmware del dispositivo de destino.

A. Productos afectados:

- SICAM A8000: Todas las versiones.
- SICAM 8: Todas las versiones.
- SICAM EGS: Todas las versiones.
- CPCI85 Procesamiento central/comunicación: antes de las 5.40.
- Sistema base SICORE: anterior a 1.4.0.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de firmware disponible que aborda estas vulnerabilidades.
- Aplicar las actualizaciones de seguridad proporcionadas utilizando las herramientas y los procedimientos documentados correspondientes que se incluyen con el producto.

Fuente de Información:	• hxxp://cert-portal.siemens.com/productcert/html/ssa-071402.html • hxxps://support.industry.siemens.com/cs/ww/en/view/109804985/ • hxxps://support.industry.siemens.com/cs/ww/en/view/109818240/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°172	Fecha: 25-07-2024 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en Docker		
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 reportado una vulnerabilidad de severidad **CRÍTICA** de tipo autorización incorrecta que afecta a ciertas versiones de Docker Engine y Docker Desktop. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante eludir los complementos de autorización (AuthZ) en determinadas circunstancias.

2. DETALLES:

El modelo de autorización predeterminado de Docker es de todo o nada. Los usuarios con acceso al demonio de Docker pueden ejecutar cualquier comando de Docker. Para un mayor control de acceso, se pueden utilizar complementos de autorización (AuthZ). Estos complementos aprueban o rechazan las solicitudes al demonio de Docker en función de la autenticación y el contexto del comando.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-41110 de tipo autorización incorrecta, podría permitir a un atacante eludir los complementos de autorización (AuthZ) en circunstancias específicas, lo que puede dar lugar a acciones no autorizadas, incluyendo la escalada de privilegios. Si bien la probabilidad de explotación es baja, el impacto podría ser significativo, lo que requiere la atención inmediata de los usuarios de Docker.

Mediante una solicitud de API especialmente diseñada, un cliente de API de Engine podría hacer que el demonio reenvíe la solicitud o la respuesta a un complemento de autorización sin el cuerpo. En determinadas circunstancias, el complemento de autorización puede permitir una solicitud que de otro modo habría denegado si se le hubiera reenviado el cuerpo.

Un atacante podría explotar una omisión mediante una solicitud de API con Content-Length establecido en 0, lo que provocaría que el demonio Docker reenvíe la solicitud sin el cuerpo al complemento AuthZ, que podría aprobar la solicitud incorrectamente.

A. Productos afectados:

- Docker Engine versiones 19.03.x y posteriores que dependen de plugins de autorización para tomar decisiones de control de acceso.
- Docker Desktop versiones anteriores a la 4.33.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Probar las actualizaciones en entornos no productivos previo al paso a producción.
- Aplicar las actualizaciones o mitigaciones pertinentes indicados por la marca a la brevedad.
- Actualizar Docker Engine y Docker Desktop a la última versión corregida lo antes posible para mitigar los riesgos potenciales.
- Deshabilitar temporalmente los complementos de AuthZ y restringir el acceso a la API de Docker si no es posible realizar una actualización de forma inmediata.

Fuente de Información:	• hxxps://www.docker.com/blog/docker-security-advisory-docker-engine-authz-plugin/ • hxxps://github.com/vvpoglazov/cve-2024-41110-checker

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°172	Fecha: 25-07-2024 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en Spring Cloud Data Flow		
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 reportado una vulnerabilidad de severidad **CRÍTICA** de tipo Limitación incorrecta de una ruta de acceso a un directorio restringido (Path Traversal) que afecta a varias versiones de Spring Cloud Data Flow anteriores a 2.11.4. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante la ejecución remota de código en Spring Cloud Data Flow.

2. DETALLES:

Spring Cloud Data Flow es una plataforma de procesamiento de datos por lotes y streaming basada en microservicios implementada en Cloud Foundry y Kubernetes. El servidor Skipper tiene la capacidad de recibir solicitudes de paquetes de carga. Existe una pequeña posibilidad, debido a una limpieza inadecuada de la ruta de carga, de que un usuario malintencionado que tenga acceso a la API del servidor Skipper pueda usar una solicitud de carga diseñada para escribir un archivo arbitrario en cualquier ubicación del sistema de archivos, lo que podría poner en riesgo el servidor.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-37084 de tipo Path Traversal, podría permitir a un atacante escribir archivos arbitrarios en cualquier ubicación del sistema de archivos, lo que puede provocar la vulneración del servidor. Un atacante puede explotar esta vulnerabilidad de forma remota a través de la red, sin necesidad de interacción ni privilegios del usuario. Esto podría dar lugar a un acceso no autorizado a datos confidenciales, la modificación de archivos críticos y la posible interrupción de las operaciones del servidor.

A. Productos afectados:

- Spring Cloud Data Flow, versiones anteriores a 2.11.4.

3. RECOMENDACIONES:

- Actualizar el producto afectado Spring Cloud Data Flow a la versión 2.11.4 o posterior lo antes posible.
- Realizar una actualización inmediata y restringir el acceso a la API del servidor Skipper sólo a los usuarios de confianza.
- Supervisar las actividades del sistema de archivos para detectar operaciones de escritura sospechosas.
- Implementar la segmentación de la red para limitar el acceso a la API del servidor Skipper.
- Auditar y revisar periódicamente los permisos del sistema de archivos para detectar cualquier cambio no autorizado.

Fuente de Información:	• hxxps://securityonline.info/cve-2024-37084-cvss-9-8-remote-code-execution-in-spring-cloud-data-flow/ • hxxps://spring.io/security/cve-2024-37084

Índice alfabético

Explotación de vulnerabilidades conocidas 6, 7, 8
Ransomware 4