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

273-2024-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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°273	Fecha: 26-11-2024 Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Ataque de ransomware afecta a Starbucks y a varios supermercados		
Tipo de Ataque	Ransomware		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:

La empresa de software detrás del sistema de pagos y programación de Starbucks ha sido víctima de un ataque de ransomware que se ha prolongado durante varios días, lo que ha provocado interrupciones que afectan el pago de los salarios.

El ataque a Blue Yonder, la empresa responsable del software, comenzó el 21 de noviembre y ha causado fallos en el sistema de Starbucks, y las cadenas de supermercados británicas Morrisons y Sainsbury's, para el seguimiento de horas trabajadas y pagos a los empleados, según informó TechCrunch.

2. DETALLES:

La violación de datos, que ocurrió el 21 de noviembre, pone de relieve los riesgos cibernéticos que enfrentan las organizaciones durante la temporada navideña de gran importancia.

Este ataque de ransomware, que tuvo como objetivo su infraestructura de servicios administrados, interrumpió las operaciones en toda su base de clientes.

Morrisons informó desafíos en la entrega fluida de productos a las tiendas, con la disponibilidad en puntos de venta mayoristas y de conveniencia cayendo hasta el 60% de los niveles normales.

Esta interrupción podría tener consecuencias graves para los compradores durante la temporada alta de las fiestas. En Estados Unidos, Starbucks confirmó que el ataque afectó a los procesos administrativos relacionados con la programación y el seguimiento del tiempo de los empleados.

Según documentos revisados por Business Insider, Starbucks ha emitido directrices a sus empleados sobre cómo manejar las interrupciones en los pagos provocadas por el fallo de Blue Yonder.

Otros clientes de Blue Yonder en los EE. UU., incluidos Kimberly-Clark, Campbell's, Wegmans y Walgreens, están monitoreando la situación de cerca mientras continúan los esfuerzos de recuperación.

Blue Yonder, conocido por ofrecer soluciones tecnológicas integrales para la gestión de cadenas de suministro, cuenta con más de 3,000 clientes en 76 países, entre ellos fabricantes, minoristas y proveedores logísticos.

En un comunicado emitido el pasado 24 de noviembre, la empresa aseguró que está trabajando en la restauración de sus servicios con el apoyo de una firma externa de ciberseguridad.

La empresa afirmó también que su entorno de nube pública Azure no se vio afectado y no se detectó ninguna actividad sospechosa.

“Hemos implementado protocolos defensivos y forenses y mantenemos a nuestros clientes informados durante toda la investigación”, dijo un portavoz de la compañía en un comunicado enviado por correo electrónico.

John Donigian, director senior de estrategia de la cadena de suministro de Moody’s, dijo que el ataque subraya cuán críticas son estas tecnologías para la gestión de la cadena de suministro global.

"Cuando estos sistemas se desconectan, se interrumpen flujos de trabajo esenciales, como la gestión de inventarios, la previsión de la demanda, la gestión de almacenes y la planificación del transporte, lo que paraliza cadenas de suministro enteras", dijo Donigian por correo electrónico. "Este incidente pone de relieve el papel indispensable que desempeñan estas tecnologías en sectores que van desde el comercio minorista hasta la logística y más allá".

Las consecuencias de un ataque a un software que forma parte de la cadena de suministro logran afectar a una amplia franja de organizaciones al apuntar a un único actor de confianza común.

3. RECOMENDACIONES:

- 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 maliciosos y otro contenido malicioso 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://gbhackers.com/blue-yonder-ransomware-attack/ • hxxps://www.businessinsider.es/tecnologia/ataque-ransomware-deja-starbucks-papel-boligrafo-controlar-horas-empleados-1425675 • hxxps://www.msn.com/es-mx/dinero/noticias/ataque-de-ransomware-afecta-operaciones-de-starbucks-y-grandes-supermercados/ar-AA1uOASm • hxxps://www.cybersecuritydive.com/news/starbucks-blue-yonder-employee-scheduling/734056/ • hxxps://www.darkreading.com/cyberattacks-data-breaches/ransomware-attack-blue-yonder-starbucks-supermarkets

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°273	Fecha: 26-11-2024 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades de inyección SQL en servidor central de Centreon		
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 dos vulnerabilidades de severidad **ALTA** de tipo inyección SQL (SQLi) que afecta a los componentes "centreon-dsm-server" y "centreon-open-tickets" del servidor central de Centreon. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado la ejecución remota de código arbitrario en los sistemas afectados.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-45755 de tipo inyección SQL en el formato para configurar ranuras de Centreon DSM, podría permitir a un usuario autenticado con acceso con privilegios elevados la inyección de SQL. La inyección de SQL puede ocurrir en el formulario para configurar las ranuras de Centreon DSM. La explotación solo es accesible para usuarios autenticados con acceso con privilegios elevados.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-45756 de tipo inyección SQL en el formato para crear un ticket en la herramienta ITSM de Centreon, podría permitir a un usuario autenticado con acceso con privilegios elevados la inyección de SQL. La inyección SQL puede ocurrir en el formulario para crear un ticket. La explotación solo es accesible para usuarios autenticados con acceso con privilegios elevados. Esta falla permite a los atacantes manipular consultas SQL mediante la inyección de datos maliciosos, lo que puede provocar un acceso o manipulación de datos no autorizados.

A. Productos afectados:

- La vulnerabilidad CVE-2024-45755 afecta al componente centreon-dsm-server (en el servidor central), versión 24.10.x anterior a 24.10.0, 24.04.x anterior a 24.04.3, 23.10.x anterior a 23.10.1, 23.04.x anterior a 23.04.3 y 22.10.x anterior a 22.10.2.
- La vulnerabilidad CVE-2024-45756 afecta al componente centreon-open-tickets (en el servidor central), versión 24.10.x anterior a 24.10.0, 24.04.x anterior a 24.04.2, 23.10.x anterior a 23.10.1, 23.04.x anterior a 23.04.3 y 22.10.x anterior a 22.10.2.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://github.com/centreon/centreon/relèase • hxxps://thewatch.centreon.com/latest-security-bulletins-64/cve-2024-45756-centreon-open-tickets-high-severity-4064 • hxxps://thewatch.centreon.com/latest-security-bulletins-64/cve-2024-45755-centreon-dsm-high-severity-4066

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°273	Fecha: 26-11-2024
		Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en dispositivos ArrayOS AG		
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:

Array Networks ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo autenticación incorrecta que afecta a los dispositivos ArrayOS AG. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario y acceder a datos confidenciales sin necesidad de autenticación.

2. DETALLES:

ArrayOS AG es un sistema operativo propietario desarrollado por Array Networks, que se utiliza principalmente en sus productos AG Series y vxAG SSL VPN. Este sistema operativo está diseñado con un fuerte énfasis en la seguridad y la confiabilidad, lo que lo hace adecuado para entornos empresariales que requieren soluciones de acceso remoto y entrega de aplicaciones seguras.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2023-28461 de tipo autenticación incorrecta en ArrayOS, podría permitir a un atacante remoto no autenticado eludir el proceso de autenticación. La vulnerabilidad existe debido a un error en el proceso de autenticación. Un atacante remoto no autenticado puede eludir el proceso de autenticación mediante una URL especialmente diseñada y obtener acceso no autorizado al dispositivo SSL-VPN.

Los atacantes pueden explotar esta vulnerabilidad enviando solicitudes HTTP diseñadas que manipulan el atributo flags en el encabezado HTTP, lo que permite el acceso no autorizado al sistema de archivos del sistema y habilita la ejecución remota de código.

la vulnerabilidad permite a los atacantes ejecutar código arbitrario en la puerta de enlace VPN SSL. Esto significa que, una vez que un atacante explota la falla, puede potencialmente tomar el control total del dispositivo VPN, comprometiendo la integridad y confidencialidad de todos los datos transmitidos a través de él.

Los atacantes pueden explorar el sistema de archivos de la puerta de enlace VPN SSL afectada. Este acceso les permite ver archivos de configuración confidenciales, registros y, posiblemente, credenciales de usuario, que pueden aprovecharse para realizar otros ataques o para la exfiltración de datos.

A. Productos afectados:

- ArrayOS AG y vxAG: versiones anteriores a 9.4.0.484.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Considerar soluciones temporales teniendo en cuenta los posibles impactos en la funcionalidad, en caso no sea posible aplicar parches de inmediato.
- Implementar soluciones de monitoreo para detectar actividades inusuales que puedan indicar intentos de explotación.
- Garantizar que existan controles de acceso y mecanismos de autenticación estrictos para todas las soluciones de acceso remoto.

Fuente de Información:	• hxxps://support.arraynetworks.net/prx/001/ • hxxp/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_Remote_Code_Execution_Vulnerability_AG.pdf

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°273	Fecha: 26-11-2024 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el compresor de archivos 7-ZIP		
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 desbordamiento de enteros en el compresor de archivos 7-ZIP. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en sistemas que ejecutan versiones vulnerables de 7-Zip explotando el proceso de descompresión Zstandard.

2. DETALLES:

7-Zip es un software gratuito de código abierto que se utiliza para comprimir y descomprimir archivos.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-11477 de tipo desbordamiento de enteros en el compresor de archivos 7-ZIP, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en las instalaciones afectadas de 7-Zip. Se requiere la interacción con esta biblioteca para explotar esta vulnerabilidad, pero los vectores de ataque pueden variar según la implementación.

La falla existe específicamente dentro de la implementación de descompresión Zstandard, donde una validación incorrecta de los datos proporcionados por el usuario puede resultar en un desbordamiento de enteros antes de escribir en la memoria. Esta vulnerabilidad permite a los atacantes ejecutar código arbitrario en el contexto del proceso actual cuando los usuarios interactúan con archivos maliciosos.

A. Productos afectados:

- x 7-Zip, todas las versiones anteriores a la 24.07.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Descargar e instalar manualmente la última versión para proteger sus sistemas, ya que el software carece de un mecanismo de actualización integrado.

Fuente de Información:	• hxxps://www.zerodayinitiative.com/advisories/ZDI-24-1532/

Índice alfabético