GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0625

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABIILIDADES	0	3	0
MALWARE	1	1	0
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Explotan vulnerabilidad en Cityworks para comprometer servidores Microsoft IIS

Recientemente se ha identificado una vulnerabilidad crítica en el software Cityworks desarrollado por Trimble, que está siendo activamente explotada por actores maliciosos. La vulnerabilidad catalogada como CVE-2025-0994, presenta un problema de deserialización que permite a usuarios autenticados ejecutar comandos de forma remota en servidores Microsoft Internet Information Services (IIS). Para dar un poco de contexto Cityworks es una solución de gestión de activos y órdenes de trabajo centrado en el Sistema de Información Geográfica (GIS), utilizada principalmente por gobiernos locales y

agencias de infraestructura para administrar activos públicos, procesar órdenes de trabajo GIS y manejar permisos y licencias.

Trimble ha confirmado que ha investigado informes de clientes sobre accesos no autorizados a sus redes mediante la explotación de esta vulnerabilidad, lo que indica que los ataques están en curso. Las versiones afectadas incluyen Cityworks anteriores a la 15.8.9 y Cityworks con Office Companion anteriores a la 23.10, Se recomienda de forma inmediata a los usuarios actualizar a las versiones más recientes para mitigar el riesgo de explotación.

Prioridad: Urgente.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/hackers-exploit-cityworks-rce-bug-to-breach-microsoft-iis-servers/

Vulnerabilidad crítica en Cisco ISE permite ejecución de comandos como Root

Cisco ha lanzado parches para corregir dos vulnerabilidades críticas en su plataforma Identity Services Engine (ISE), identificadas como CVE-2025-20124 y CVE-2025-20125. Estas fallas pueden ser explotadas por atacantes remotos autenticados con privilegios de administrador de solo lectura para ejecutar comandos arbitrarios con privilegios de root y eludir la autorización en dispositivos no actualizados, Ambas vulnerabilidades afectan a Cisco ISE y al Conector de Identidad Pasiva de Cisco ISE (ISE-PIC), independientemente de la configuración del dispositivo.

La vulnerabilidad CVE-2025-20124 se debe a una deserialización insegura de flujos de bytes Java proporcionados por el usuario, un atacante podría explotarla enviando un objeto Java serializado manipulado a una API afectada, lo que le permitiría ejecutar comandos arbitrarios en el dispositivo y elevar privilegios. Por otro lado, la CVE-2025-20125 surge de una falta de autorización en una API específica y una validación inadecuada de los datos proporcionados por el usuario, esto puede ser explotado mediante solicitudes HTTP

maliciosas para obtener información, modificar la configuración del sistema vulnerable y reiniciar el dispositivo, Se recomienda a los administradores migrar o actualizar sus dispositivos Cisco ISE a las versiones corregidas lo antes posible para mitigar estos riesgos.

Prioridad: Urgente.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/critical-cisco-ise-bug-can-let-attackers-run-commands-as-root/

Grupos de ciberdelincuencia explotan vulnerabilidad en 7-Zip para eludir protecciones de Windows

Recientemente se ha detectado que grupos de ciberdelincuentes están explotando una vulnerabilidad en la herramienta de compresión 7-Zip, identificada como CVE-2025-0411, esta vulnerabilidad permite a los atacantes eludir la protección "Marca de la Web" (Mark of the Web, MotW) de Windows y ejecutar código arbitrario en el contexto del usuario actual, La explotación se lleva a cabo mediante campañas de phishing dirigidas, donde se utilizan archivos adjuntos que aparentan ser documentos legítimos pero que en realidad contienen archivos maliciosos doblemente comprimidos.

Para mitigar este riesgo, se recomienda a los usuarios actualizar 7-Zip a la versión 24.09 o posterior, donde la vulnerabilidad ha sido corregida. Además, es aconsejable implementar filtros de correo electrónico para bloquear intentos de phishing y deshabilitar la ejecución de archivos provenientes de fuentes no confiables, estas medidas ayudarán a prevenir posibles infecciones y protegerán los sistemas contra este tipo de ataques.

Prioridad: Urgente.

Ampliar Información:

https://thehackernews.com/2025/02/russian-cybercrime-groups-exploiting-7.html

Recomendaciones generales sobre vulnerabilidades:

Para mitigar las vulnerabilidades en los sistemas, se recomiendan las siguientes medidas claves.

1. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.
2. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.
3. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.
4. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.
5. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

Sitios falsos de Google Chrome distribuyen el malware ValleyRAT

Actores de ciberamenazas conocidos como Silver Fox, están distribuyendo el troyano de acceso remoto ValleyRAT a través de sitios web falsos que imitan al navegador Google Chrome. El malware es propagado mediante la descarga de un archivo comprimido ZIP que contiene un ejecutable malicioso, al ejecutar este archivo se cargan DLLs adicionales que a su vez se infiltran en programas legítimos como Douyin, lo que permite al malware mantenerse oculto y persistente en el sistema, ValleyRAT permite a los atacantes realizar un seguimiento de la pantalla de la víctima, registrar pulsaciones de teclas y acceder a información confidencial.

El malware fue identificado por expertos en seguridad y ha afectado a usuarios principalmente en regiones de china, como Hong Kong, Taiwán e incluso en latino américa. Para evitar ser víctimas de este tipo de ataques, se recomienda a los usuarios verificar la autenticidad de los sitios web antes de descargar cualquier software y mantener actualizado su antivirus para detectar y bloquear archivos maliciosos. Además, deben evitar hacer clic en enlaces sospechosos y en anuncios que ofrezcan descargas rápidas o gratuitas.

Prioridad: Urgente.

Ampliar Información:

https://thehackernews.com/2025/02/fake-google-chrome-sites-distribute.html

---

Abuso de la delegación de Kerberos en Active Directory: riesgo en redes empresariales

Se ha identificado una técnica de ataque que explota la delegación de Kerberos sin restricciones en redes de Active Directory (AD), este malware permite a los atacantes escalar privilegios y comprometer toda la infraestructura de un dominio, el ataque se aprovecha de la capacidad de los servicios para suplantar a usuarios a través de la delegación de Kerberos, una función que facilita el acceso a recursos dentro de una red. Este tipo de malware activa una vulnerabilidad que ha sido conocida por algún tiempo, pero sigue siendo una preocupación crítica debido a la prevalencia de sistemas que aún utilizan configuraciones heredadas de Kerberos, como la delegación sin restricciones, que Microsoft introdujo en versiones anteriores de Windows Server.

El malware o la explotación de esta vulnerabilidad se facilita a través de una configuración deficiente en los sistemas de autenticación de Windows, permitiendo a los atacantes moverse lateralmente por la red y obtener acceso a servicios de alto nivel. Para mitigar este riesgo, se recomienda actualizar los sistemas a configuraciones más seguras, como la

delegación restringida o basada en recursos, y también colocar cuentas de alto privilegio en grupos protegidos. Además, se aconseja revisar y reforzar las configuraciones de SPN y habilitar controles de acceso más estrictos para prevenir el uso malicioso de estas funciones.

Prioridad: Critico.

Ampliar Información:

https://cybersecuritynews.com/abusing-kerberos-delegation-in-active-directory/

Recomendaciones generales sobre malware

Para protegerse contra malware, es esencial:

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.
2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

Interrupción de Cloudflare causada por bloqueo erróneo de URL de phishing

El 6 de febrero de 2025, Cloudflare experimentó una interrupción significativa de 59 minutos en sus servicios debido a un error al intentar bloquear una URL de phishing en su plataforma

de almacenamiento de objetos R2. En lugar de bloquear el punto final específico asociado con el informe de abuso, un empleado desactivó accidentalmente todo el servicio R2 Gateway, afectando múltiples servicios, incluyendo Stream, Images, Cache Reserve y Vectorize.

Para prevenir incidentes similares en el futuro, Cloudflare ha reconocido la necesidad de mejorar los controles del sistema y la capacitación de los operadores, la empresa ha implementado medidas correctivas para evitar que errores humanos afecten la disponibilidad de sus servicios.

Prioridad: Importante.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/cloudflare-outage-caused-by-botched-blocking-of-phishing-url/

Microsoft comparte solución temporal para problemas de actualización de seguridad en Windows

Microsoft ha identificado un problema que impide la instalación de actualizaciones de seguridad en algunos sistemas con Windows 11 versión 24H2, este inconveniente ocurre cuando se instala Windows 11 desde medios como CDs o USBs que incluyen las actualizaciones acumulativas de octubre o noviembre de 2024. La compañía ha proporcionado una solución temporal para los usuarios afectados recomendando que no se utilicen estos medios de instalación específicos para evitar el problema.

Para resolver la situación, Microsoft sugiere que los usuarios reinstalen Windows 11 versión 24H2 utilizando medios de instalación que incluyan actualizaciones de seguridad posteriores a diciembre de 2024, esta medida garantizará que los sistemas puedan recibir e instalar correctamente las actualizaciones de seguridad necesarias, es importante

destacar que este problema no afecta a las actualizaciones de seguridad entregadas a través de Windows Update o el Catálogo de Actualizaciones de Microsoft.

Prioridad: Importante.

Ampliar Información:

https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-workaround-for-windows-security-update-issues/