GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1525

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	2	1
MALWARE	0	1	1
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Vulnerabilidad en el servicio IPsec IKEv1

Fortinet ha divulgado una vulnerabilidad de severidad baja (CVE-2024-46669) en su sistema operativo FortiOS y FortiSASE FortiOS tenant, específicamente relacionada con un desbordamiento de enteros en el servicio IPsec IKEv1 cuando se accede a través de la interfaz de línea de comandos (CLI). Esta falla, identificada en el boletín FG-IR-24-267, podría ser explotada para provocar un comportamiento inesperado en el sistema afectado, aunque no se considera crítica ni fácilmente explotable.

La compañía recomienda a sus usuarios revisar las versiones afectadas y aplicar las actualizaciones de seguridad correspondientes para mitigar el riesgo. Aunque el impacto es limitado, mantener los sistemas actualizados es esencial para preservar la integridad y estabilidad de la infraestructura. Fortinet ha puesto a disposición parches correctivos a través de sus canales oficiales.

Prioridad: Importante.

Ampliar Información:

https://www.fortiguard.com/psirt/FG-IR-24-267

Fallo en validación de certificado en conexión FGFM

Fortinet ha identificado una vulnerabilidad de severidad media en FortiOS y FortiProxy, relacionada con la verificación inadecuada del nombre del certificado en las conexiones FGFM (FortiGate to FortiManager). Esta falla, documentada en el boletín FG-IR-24-046, podría permitir que un atacante con acceso a la red intercepte o manipule comunicaciones entre dispositivos, comprometiendo la integridad y confidencialidad de los datos transmitidos.

Para mitigar este riesgo, se recomienda a los administradores de sistemas que actualicen a las versiones corregidas proporcionadas por Fortinet. Además, es fundamental revisar las configuraciones de seguridad y aplicar las mejores prácticas para asegurar las comunicaciones entre dispositivos en la red.

Prioridad: Urgente.

Ampliar Información:

https://www.fortiguard.com/psirt/FG-IR-24-046

Vulnerabilidad NTLM de Windows

Una vulnerabilidad crítica en Microsoft Windows, identificada como CVE-2025-24054, permite la filtración de hashes NTLMv2-SSP mediante archivos.library-ms maliciosos. Esta falla puede ser explotada sin que el usuario ejecute el archivo, ya que solo con visualizarlo o interactuar con él (como al hacer clic derecho) se activa el envío de credenciales al

atacante. Esto facilita ataques de relay NTLM y posibles escalaciones de privilegios en redes internas.

Aunque Microsoft lanzó un parche el 11 de marzo de 2025, actores maliciosos ya estaban explotando esta falla en campañas dirigidas, particularmente en Europa del Este. Se han utilizado archivos comprimidos que contienen referencias a servidores SMB maliciosos controlados por los atacantes. Se recomienda aplicar de inmediato las actualizaciones de seguridad y revisar las configuraciones de red y compartición de archivos para mitigar el riesgo.

Prioridad: Urgente.

Ampliar Información:

https://gbhackers.com/windows-ntlm-vulnerability/

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

Midnight Blizzard implementa el nuevo malware GrapeLoader

El grupo de ciberespionaje ruso Midnight Blizzard (también conocido como APT29 o Cozy Bear) ha desplegado una nueva campaña de phishing dirigida a embajadas y entidades diplomáticas europeas desde enero de 2025. Utilizando correos que aparentan ser invitaciones a eventos de cata de vinos, los atacantes distribuyen archivos ZIP que incluyen un ejecutable legítimo de PowerPoint, una DLL y el malware GrapeLoader. Este se activa mediante DLL sideloading para recolectar información del sistema, establecer persistencia y conectarse a servidores de comando y control.

Una vez desplegado, GrapeLoader descarga WineLoader, un backdoor modular diseñado para extraer datos como dirección IP, nombre de usuario y privilegios. Esta versión de WineLoader incorpora técnicas avanzadas de evasión, como la ofuscación del código y cargas en memoria, lo que complica su detección. Esta campaña demuestra la sofisticación creciente del grupo y la necesidad de reforzar los controles de seguridad, especialmente en organizaciones gubernamentales y diplomáticas.

Prioridad: Importante.

https://www.bleepingcomputer.com/news/security/midnight-blizzard-deploys-new-grapeloader-malware-in-embassy-phishing/

Nuevo malware ResolverRAT ataca a sector salud y farmacéutico global

Un nuevo malware denominado ResolverRAT ha sido identificado como parte de campañas dirigidas contra organizaciones del sector farmacéutico y sanitario a nivel mundial. Este troyano de acceso remoto se distribuye mediante correos electrónicos de phishing personalizados según el idioma del país objetivo, que simulan violaciones legales o de derechos de autor. El malware se ejecuta aprovechando la técnica de DLL sideloading a través de archivos ejecutables legítimos que inyectan el código malicioso en memoria.

ResolverRAT está diseñado para operar de forma sigilosa, cargando ensamblados maliciosos en memoria sin invocar funciones de API detectables, y emplea avanzadas técnicas de evasión como ofuscación del flujo de control y detección de entornos de análisis. Para mantener persistencia, realiza modificaciones en el registro y se replica en distintos directorios del sistema. Además, utiliza comunicaciones cifradas con autenticación basada en certificados, rotación de direcciones IP, y técnicas de exfiltración fragmentada para evadir controles de seguridad.

Prioridad: Urgente.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/new-resolverrat-malware-targets-pharma-and-healthcare-orgs-worldwide/

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

Microsoft corrige fallos críticos en Office 2016

Microsoft lanzó una actualización de emergencia para resolver errores introducidos por un parche anterior que provocaba cierres inesperados en Word, Excel y Outlook en instalaciones de Office 2016. Los problemas fueron reportados tras la instalación de una actualización de seguridad reciente que afectó a múltiples usuarios.

La nueva corrección está dirigida a versiones de Office 2016 basadas en Microsoft Installer (MSI) y debe aplicarse junto al parche previo para restaurar completamente la funcionalidad. Además, se solucionaron errores en los enlaces de descarga de versiones localizadas de Outlook que redirigían incorrectamente a la versión en inglés.

Prioridad: Importante.

Ampliar Información:

https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-emergency-update-to-fix-office-2016-crashes/

La mayoría de las extensiones de navegador pueden acceder a información confidencial empresarial

Un reciente análisis evidenció que el 99% de los empleados en entornos corporativos utilizan extensiones de navegador, y más del 50% de estas tienen permisos que permiten acceso a información sensible como contraseñas, cookies y datos del contenido web. Esto representa una amenaza significativa para la seguridad organizacional, especialmente ante el crecimiento del uso de extensiones con capacidades de inteligencia artificial.

El estudio también reveló que una parte importante de las extensiones no han sido actualizadas en más de un año y que muchas son desarrolladas por usuarios anónimos o

con correos genéricos, dificultando su validación. Se recomienda a las organizaciones establecer controles sobre el uso de extensiones y realizar auditorías periódicas para mitigar riesgos de fuga o abuso de información.

Prioridad: Importante.

Ampliar Información:

https://thehackernews.com/2025/04/majority-of-browser-extensions-can.html

---