GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0525

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

VULNERABILIDADES

Falla crítica en Routers D-Link permite control remoto

Se ha identificado una vulnerabilidad crítica de ejecución remota de código (RCE) en los routers D-Link DSL-3788, permitiendo a atacantes tomar el control total del dispositivo. La falla, causada por una validación inadecuada en la función "COMM_MakeCustomMsg", fue corregida en la versión de firmware v1.01R1B037. D-Link insta a los usuarios a actualizar sus dispositivos de inmediato para mitigar riesgos de seguridad y privacidad.

Prioridad: Crítico

Ampliar información:

https://gbhackers.com/critical-d-link-router-flaw/

Vulnerabilidad en objetos COM de Windows permite ejecución remota de código

Investigadores de Google Project Zero han identificado una vulnerabilidad crítica en objetos COM de Windows que permite la ejecución remota de código y escalada de privilegios. Este problema surge del uso inapropiado de tecnologías de remoting como DCOM y .NET Remoting, que exponen objetos inseguros a través de límites de seguridad, permitiendo a los atacantes ejecutar código malicioso en el contexto de procesos protegidos. Aunque Microsoft ha implementado algunas mitigaciones, como validaciones más estrictas en Windows 11, la vulnerabilidad sigue siendo un riesgo significativo, lo que resalta la importancia de validar adecuadamente los objetos remotos en entornos de alta seguridad.

Prioridad: Crítico

Ampliar información:

https://gbhackers.com/windows-com-object-vulnerability-enables-remote-code-execution/

Vulnerabilidad en GitHub Copilot explotada para entrenar modelos de IA maliciosos

GitHub Copilot, la herramienta de autocompletado impulsada por IA, ha sido objeto de críticas tras el descubrimiento de dos vulnerabilidades por parte de Apex Security. La primera vulnerabilidad permite eludir los filtros éticos de Copilot al iniciar las consultas con la palabra “Sure”, lo que lleva al asistente a proporcionar respuestas sobre tareas éticamente cuestionables, como inyecciones SQL o la creación de redes Wi-Fi falsas. La segunda vulnerabilidad, relacionada con la configuración de proxies, permite el acceso no autorizado a modelos avanzados de OpenAI, lo que elimina restricciones y requisitos de facturación, ofreciendo acceso gratuito a potentes recursos de IA.

Prioridad: Importante

Ampliar información:

https://gbhackers.com/github-copilot-vulnerability-exploited/

Vulnerabilidad en los controladores de pantalla NVIDIA GPU permite acceso remoto a archivos

NVIDIA ha lanzado una actualización de seguridad crítica para abordar múltiples vulnerabilidades en su controlador de pantalla GPU y software vGPU, que afectan tanto a sistemas Windows como Linux. Entre estas vulnerabilidades, CVE-2024-0149, que afecta al controlador de pantalla GPU de NVIDIA para Linux, podría permitir el acceso no autorizado a archivos. Las vulnerabilidades, que fueron divulgadas en enero de 2025, pueden permitir denegación de servicio (DoS), manipulación de datos, divulgación de información e incluso ejecución remota de código. Se recomienda a los usuarios actualizar sus controladores a través de la página de descargas de NVIDIA o el portal de licencias de vGPU para mitigar estos riesgos.

Prioridad: Urgente

Ampliar información:

https://gbhackers.com/nvidia-gpu-display-drivers-vulnerability/

TeamViewer Corrige vulnerabilidad crítica de elevación de privilegios en aplicaciones de Windows

TeamViewer ha corregido una vulnerabilidad crítica (CVE-2025-0065) en sus aplicaciones cliente y host para Windows, que permitía a un atacante con acceso local inyectar argumentos en el componente 'TeamViewer_service.exe' y elevar sus privilegios. Esta falla

afectaba a las versiones 11.x a 15.x del software, y fue solucionada con las actualizaciones de las versiones 15.62, 14.7.48799, 13.2.36226, 12.0.259319 y 11.0.259318. Aunque no se ha detectado explotación en el entorno real, se recomienda a los usuarios actualizar sus aplicaciones para prevenir posibles abusos, ya que las herramientas de acceso remoto como TeamViewer han sido objeto de ataques previos para cargar malware y establecer acceso remoto no autorizado.

Prioridad: Urgente

Ampliar información:

https://www.securityweek.com/teamviewer-patches-high-severity-vulnerability-in-windows-applications/

Recomendaciones generales sobre vulnerabilidades:

Aplique siempre los parches de seguridad más recientes proporcionados por los fabricantes para corregir vulnerabilidades críticas y mitigar riesgos de explotación.

Implemente sistemas de monitoreo para detectar actividades sospechosas, como accesos no autorizados o cambios no autorizados en configuraciones críticas. Configure alertas para comportamientos anómalos que puedan indicar la explotación de vulnerabilidades.

Aplique controles de acceso basados en roles (RBAC) y realice segmentación de red para limitar el impacto en caso de que una vulnerabilidad sea explotada en un sistema.

Limite el acceso a servicios no utilizados, cierre puertos innecesarios y restrinja el acceso solo a usuarios y redes confiables para reducir la exposición a ataques.

Realice pruebas de penetración y auditorías de seguridad periódicas para identificar vulnerabilidades no reportadas o posibles brechas en la infraestructura

MALWARE

TorNet Backdoor: nueva amenaza que usa tareas programadas para propagar malware

Investigadores de Cisco Talos han identificado una campaña activa desde 2024 que utiliza el backdoor TorNet para infectar sistemas Windows mediante correos de phishing dirigidos a usuarios en Polonia y Alemania. El malware emplea PureCrypter para evadir detección y cargar cargas adicionales como Agent Tesla y Snake Keylogger. TorNet usa la red TOR para ocultar su tráfico y ejecuta tareas programadas para persistencia, dificultando su eliminación. Se recomienda implementar defensas avanzadas y monitoreo continuo para mitigar el riesgo.

Prioridad: Urgente

Ampliar información:

https://gbhackers.com/tornet-backdoor-exploits-windows-scheduled-tasks/

Tria Stealer: malware para Android roba mensajes de WhatsApp

Investigadores han detectado la campaña de malware Tria Stealer, activa desde 2024, que engaña a usuarios en Malasia y Brunei con falsas invitaciones de boda para instalar aplicaciones maliciosas. El malware roba SMS, correos y mensajes de WhatsApp, utilizando bots de Telegram para enviar los datos a los atacantes, permitiéndoles secuestrar cuentas y realizar fraudes. Se oculta como una app de configuración y usa permisos abusivos para monitorear notificaciones y llamadas. Se recomienda evitar instalar APKs de fuentes no verificadas y reforzar la seguridad de los dispositivos.

Prioridad: **Importante**

Ampliar información:

https://gbhackers.com/new-android-malware-exploiting-wedding-invitations/

Coyote Banking Malware Abusa de Archivos LNK para Desplegar Ataques

Investigadores de FortiGuard Labs han identificado el troyano bancario Coyote, que utiliza archivos LNK maliciosos para ejecutar scripts de PowerShell y desplegar cargas útiles que roban credenciales bancarias de más de 70 aplicaciones financieras. El malware emplea keylogging, captura de pantallas y superposiciones de phishing, y se comunica con servidores C2 para recibir comandos, lo que le permite evadir medidas de seguridad y mantener persistencia. Se recomienda actualizar los antivirus y evitar ejecutar accesos directos sospechosos.

Prioridad: **Urgente**

Ampliar información:

https://gbhackers.com/coyote-banking-malware-abusing-windows-lnk-files/

Recomendaciones generales sobre malware:

Asegúrese de que los sistemas de detección de amenazas y antivirus estén actualizados para detectar malware conocido y prevenir ataques.

No descargue software ni abra enlaces de correos electrónicos o sitios web desconocidos. Fomente el uso exclusivo de repositorios oficiales para minimizar el riesgo de infecciones.

Eduque a los empleados y usuarios sobre cómo identificar intentos de phishing y engaños en línea, ya que muchos ataques de malware se inician a través de técnicas de ingeniería social.

Limite los privilegios de usuario y evite que los empleados instalen o ejecuten software no autorizado en sus sistemas corporativos para reducir la superficie de ataque.

Monitoree el tráfico de red de manera continua para detectar actividades sospechosas, como conexiones a servidores remotos desconocidos, lo que podría indicar que un sistema ha sido comprometido.

NOTICIAS DE CIBERSEGURIDAD

cibercriminales explotan infraestructura de GitHub para distribuir Lumma Stealer

Un reciente análisis de Trend Micro ha revelado una sofisticada campaña de malware que utiliza la infraestructura de GitHub para distribuir Lumma Stealer, SectopRAT, Vidar y Cobeacon. Los atacantes aprovechan URLs seguras temporales en los repositorios de GitHub para distribuir binarios maliciosos, como Pictore.exe, que exfiltran información sensible y establecen conexiones con servidores de comando y control. Los archivos maliciosos, firmados con certificados revocados, emplean scripts de PowerShell para evitar la detección y mantener la persistencia. Esta campaña muestra la evolución de las tácticas de los atacantes al utilizar plataformas confiables para distribuir malware de manera más efectiva, utilizando un enfoque modular para implementar múltiples familias de malware y evadir las defensas de seguridad.

Prioridad: Importante

Ampliar información:

https://gbhackers.com/cybercriminals-exploit-github-infrastructure/