GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0325

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	1	4	0
MALWARE	0	2	0
NOTICIAS DE CIBERSEGURIDAD	0	2	1

VULNERABILIDADES

Hackers explotan vulnerabilidad de día cero en Fortinet para obtener privilegios de superadministrador

Una vulnerabilidad de día cero en los productos FortiOS y FortiProxy de Fortinet, identificada como CVE-2024-55591, está siendo explotada activamente por atacantes para obtener privilegios de superadministrador. El fallo, ubicado en el módulo websocket de Node.js, permite la ejecución remota de código mediante solicitudes manipuladas. Los ataques, detectados inicialmente por Arctic Wolf, incluyen creación de cuentas no autorizadas, cambios en la configuración y movimientos laterales. Fortinet recomienda actualizar a las versiones parcheadas más recientes y, como medida temporal, deshabilitar interfaces administrativas HTTP/HTTPS o restringir el acceso a estas.

Prioridad: Crítico

Ampliar información:

https://gbhackers.com/hackers-exploiting-fortinet-zero-day-vulnerability/

SAP corrige fallos críticos en NetWeaver que permitían acceso no autorizado

SAP abordó 14 vulnerabilidades en su actualización de seguridad de enero de 2025, incluyendo dos fallos críticos en SAP NetWeaver identificados como CVE-2025-0070 y CVE-2025-0066, ambos con una puntuación CVSS de 9.9. Estas fallas permitían a atacantes comprometer la autenticidad, confidencialidad e integridad del sistema. También se solucionaron otras vulnerabilidades importantes, como una inyección SQL (CVE-2025-0063) y un fallo de secuestro de DLL (CVE-2025-0069). Se insta a los usuarios a aplicar las actualizaciones de inmediato para proteger sistemas críticos de posibles ataques.

Prioridad: Urgente

Ampliar información:

https://gbhackers.com/critical-sap-netweaver-flaws/

Nvidia, Zoom y Zyxel corrigen vulnerabilidades de alta gravedad

Nvidia, Zoom y Zyxel han lanzado parches para corregir varias vulnerabilidades de alta gravedad en sus productos. Nvidia solucionó tres defectos en Container Toolkit y GPU Operator para Linux, incluyendo dos fallos de aislamiento incorrecto (CVE-2024-0135 y CVE-2024-0136), que podrían permitir la ejecución remota de código y la escalada de privilegios. Zoom corrigió un problema de confusión de tipo (CVE-2025-0147) en la aplicación Workplace para Linux, que podría permitir a los atacantes escalar privilegios. Zyxel solucionó una vulnerabilidad en la gestión de privilegios (CVE-2024-12398) en 23 modelos de puntos de acceso y routers, que permitía a usuarios autenticados con privilegios limitados escalar a privilegios de dministrador.

Prioridad: Urgente

Ampliar información:

https://www.securityweek.com/nvidia-zoom-zyxel-patch-high-severity-vulnerabilities/

Adobe corrige vulnerabilidades críticas de ejecución remota de código en Photoshop

Adobe lanzó parches para más de una docena de vulnerabilidades de seguridad en varios productos, incluidos Photoshop, Substance 3D Stager, Illustrator para iPad, Adobe Animate y Adobe Substance 3D Designer. Las vulnerabilidades más graves incluyen fallos de ejecución arbitraria de código en Photoshop (CVE-2025-21127 y CVE-2025-21122), así como defectos de seguridad de memoria en Substance 3D Stager, Illustrator para iPad y Substance 3D Designer. Estos fallos podrían ser explotados por atacantes para ejecutar código malicioso en los sistemas afectados, y se recomienda a los usuarios actualizar inmediatamente.

Prioridad: Urgente

Ampliar información:

https://www.securityweek.com/adobe-critical-code-execution-flaws-in-photoshop/

Microsoft corrige tres vulnerabilidades críticas de Windows Hyper-V explotadas

Microsoft lanzó su actualización de Patch Tuesday para enero de 2025, abordando 160 vulnerabilidades, incluida una serie de tres fallos de escalamiento de privilegios en la plataforma Windows Hyper-V, ya explotados activamente. Estos defectos, identificados como CVE-2025-21334, CVE-2025-21333 y CVE-2025-21335, afectan al

servicio de virtualización NT Kernel Integration VSP y pueden permitir a los atacantes obtener privilegios de sistema. Además, Microsoft corrigió 12 vulnerabilidades críticas, muchas de las cuales pueden ser explotadas para ejecutar código de forma remota en servicios como Remote Desktop y Microsoft Excel.

Prioridad: Urgente

Ampliar información:

https://www.securityweek.com/microsoft-patches-trio-of-exploited-windows-hyper-v-zero-days/

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

Ataque de malware WP3.XYZ compromete 5,000 sitios de WordPress

Una campaña de malware identificada como WP3.XYZ ha afectado a 5,000 sitios de WordPress, explotando vulnerabilidades aún no determinadas. El ataque utiliza scripts maliciosos para crear cuentas administrativas no autorizadas y activar un plugin malicioso que exfiltra datos sensibles a un servidor remoto. La técnica emplea tokens CSRF para subir plugins infectados y obfusca las transmisiones para evadir detección. Los sitios comprometidos presentan referencias al dominio malicioso wp3[.]xyz. Como mitigación, se recomienda bloquear dominios maliciosos en firewalls y eliminar usuarios y plugins sospechosos. Se recomienda auditar regularmente los sistemas de WordPress.

Prioridad: Urgente

Ampliar información:

https://gbhackers.com/5000-wordpress-sites-hacked/

Ataques a aplicaciones PHP comprometen miles de plataformas en Indonesia

Una campaña sofisticada descubierta por Imperva ha explotado vulnerabilidades en miles de aplicaciones web basadas en PHP, con un enfoque en plataformas relacionadas con apuestas en Indonesia. Los ataques emplean bots basados en Python y webshells para instalar la herramienta de red GSocket, que permite acceso remoto no autorizado. Moodle, un sistema popular de gestión de aprendizaje, ha sido uno de los principales objetivos. Los sitios comprometidos redirigen tráfico a páginas de apuestas como "pktoto[.]cc" utilizando PHP malicioso.

Prioridad: **Urgente**

Ampliar información:

https://gbhackers.com/php-based-web-applications-exploited/

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 de clic sobre enlaces provenientes 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

"Star Blizzard" explota cuentas de WhatsApp mediante códigos QR

Microsoft Threat Intelligence identificó un cambio estratégico del grupo ruso Star Blizzard, conocido por ataques de phishing dirigidos. Desde noviembre de 2024, han utilizado WhatsApp como vector, enviando correos con códigos QR falsos que redirigen a páginas

de phishing. Estos atacan la función de vinculación de dispositivos de WhatsApp, otorgando a los hackers acceso no autorizado a mensajes y datos sensibles.

Prioridad: Urgente

Ampliar información:

https://gbhackers.com/exploit-whatsapp-accounts-using-qr-codes/

Nuevo módulo de IA detecta contenido malicioso en Telegram

Un desarrollador ruso, con apoyo de la Iniciativa Nacional de Tecnología, presentó el módulo de IA "Apparatus Sapiens" para monitorear y analizar contenido en Telegram. La herramienta examina chats abiertos y cerrados, identificando actividad delictiva con rapidez y precisión. Además, permite desanonimizar autores y recopilar datos como números telefónicos y ubicaciones, compartidos con autoridades bajo acuerdos legales. Mientras se destaca su potencial contra el ciberdelito, expertos advierten sobre posibles usos indebidos, como acoso o extorsión. Esta innovación subraya el desafío de equilibrar seguridad y privacidad en la lucha contra el crimen digital.

Prioridad: Importante

Ampliar información:

https://gbhackers.com/new-tool-unveiled-to-scan-hacking-content/

Vulnerabilidad en ChatGPT Crawler utilizada para lanzar ataques DDoS

Investigadores de seguridad han descubierto una grave vulnerabilidad en la API de ChatGPT de OpenAI, que permite a los atacantes explotarla para iniciar ataques DDoS reflexivos. El defecto, con una puntuación CVSS de 8.6, se debe a la falta de validación en las solicitudes HTTP POST enviadas a https://chatgpt.com/backend-api/attributions. Los

atacantes pueden incluir miles de URLs en una sola solicitud, lo que provoca que el servidor de ChatGPT envíe peticiones simultáneas a un sitio web objetivo desde múltiples direcciones IP, abrumando el servidor y causando posibles interrupciones en el servicio. La vulnerabilidad no afecta la confidencialidad ni la integridad de los datos, pero puede resultar en daños significativos a la disponibilidad de los sitios web atacados.

Prioridad: Urgente

Ampliar información:

https://gbhackers.com/chatgpt-crawler-vulnerability/
