GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0324

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	3	4	
MALWARE		3	1
NOTICIAS DE CIBERSEGURIDAD		2	1

VULNERABILIDADES

CISA alerta sobre la explotación activa de una vulnerabilidad crítica en Microsoft SharePoint

La Agencia de Ciberseguridad e Infraestructura de Estados Unidos (CISA) ha emitido una alerta sobre una vulnerabilidad de seguridad crítica que está siendo activamente explotada en Microsoft SharePoint Server, identificada como CVE-2023-29357 con una puntuación de CVSS de 9.8. Esta falla, que permite la escalada de privilegios, permite a los atacantes obtener privilegios de administrador al explotar tokens de autenticación JSON Web Token (JWT) falsificados.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2024/01/act-now-cisa-flags-active-exploitation.html

Principales empresas publican parches de seguridad en el primer martes de actualizaciones de 2024

Intel, AMD, Zoom y Splunk han lanzado parches de seguridad para abordar vulnerabilidades en sus productos. Intel solucionó problemas en el firmware BIOS de NUC, mientras que AMD no tiene prevista ninguna mitigación para un asunto de baja gravedad en SEV-SNP. Splunk atendió múltiples vulnerabilidades en sus soluciones de seguridad, y Zoom corrigió una vulnerabilidad de escalada de privilegios.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/intel-amd-zoom-splunk-release-patch-tuesday-security-advisories/

Actualización de seguridad de Android - enero 2024

Google lanzó la primera actualización de seguridad para Android en 2024, abordando 58 vulnerabilidades en la plataforma, incluyendo problemas en componentes críticos como el Framework y System. La actualización soluciona defectos de gravedad alta, como la elevación de privilegios y divulgación de información. Se recomienda a los usuarios que actualicen sus dispositivos para mitigar posibles riesgos.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/androids-january-2024-security-update-patches-58-vulnerabilities/

Actualización de seguridad de Adobe para Substance 3D Stager

Adobe ha lanzado parches para seis defectos de seguridad en su producto Substance 3D Stager. Estas vulnerabilidades, calificadas como de "importancia", pueden ser aprovechadas por atacantes para llevar a cabo ejecuciones de código. Se insta a los usuarios de macOS y Windows a aplicar las actualizaciones de inmediato y se recomienda la actualización a la versión 2.1.4 de Substance 3D Stager para mitigar problemas de seguridad de memoria.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/adobe-patches-code-execution-flaws-in-substance-3d-stager/

Splunk Parchea Vulnerabilidades Críticas en Enterprise Security

Splunk ha solucionado varias vulnerabilidades críticas en Splunk Enterprise Security y Splunk User Behavior Analytics (UBA) relacionadas con paquetes de terceros. Las vulnerabilidades, con calificaciones de severidad entre 7.1 (Alta) y 9.8 (Crítica), afectaban a bibliotecas como babel/traverse, handsontable y json5. Se recomienda a los usuarios actualizar a las versiones 7.3.0, 7.2.0 o 7.1.2 para evitar posibles explotaciones.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/splunk-patched-critical-vulnerabilities/

Vulnerabilidades de alto riesgo en Productos QNAP

QNAP ha abordado múltiples vulnerabilidades de alto, medio y bajo riesgo en varios productos, incluyendo QTS, QuTS hero, Netatalk, Video Station, QuMagie y QcalAgent. Las CVE asociadas afectan

a diversas versiones de los productos y abarcan categorías como inyección SQL, ejecución remota de código y más. Se recomienda a los usuarios afectados que apliquen las actualizaciones correspondientes para mitigar estos riesgos.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/multiple-qnap-high-severity-flaws/

Vulnerabilidad crítica de ejecución remota de código descubierta en firewalls Juniper SRX y Switches EX

Juniper Networks ha lanzado actualizaciones críticas para abordar una vulnerabilidad de ejecución remota de código en sus firewalls SRX Series y switches EX Series. La vulnerabilidad, clasificada como CVE-2024-21591, con una puntuación CVSS de 9.8, podría permitir a un atacante no autenticado causar una denegación de servicio o ejecución remota de código, obteniendo así privilegios de root en el dispositivo. Se recomienda a los usuarios aplicar las actualizaciones correspondientes o implementar medidas temporales, como deshabilitar J-Web o restringir el acceso a hosts de confianza.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2024/01/critical-rce-vulnerability-uncovered-in.html

---

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y aplicaciones actualizados conforme a información directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se pueden aplicar las actualizaciones de inmediato.

- Establecer una política y un plan periódico de mitigación de vulnerabilidades.
- Utilizar soluciones de gestión de vulnerabilidades para priorizar y abordar las vulnerabilidades.
- Adquirir tecnologías para bloquear accesos maliciosos y explotaciones de vulnerabilidades conocidas y de día cero.
- Utilizar servicios de Ethical Hacking para identificar posibles superficies de ciberataque y proteger los datos sensibles.
- Implementar sistemas de detección de intrusiones, sistemas de prevención de pérdida de datos y firewalls de aplicaciones web.
- Realizar auditorías de seguridad y pruebas de penetración regularmente.
- Educar a los usuarios y al personal de TI sobre las mejores prácticas de seguridad cibernética.
- Establecer políticas de seguridad sólidas, como el uso de contraseñas seguras y la gestión adecuada de accesos y privilegios.

MALWARE

SpectralBlur: nuevo backdoor en macOS

SpectralBlur, un nuevo backdoor en macOS, ha sido vinculado a la familia de malware KandyKorn utilizada por el grupo de piratería norcoreano Lazarus. Aunque desarrollados por diferentes actores, ambos comparten similitudes en sus capacidades y funciones. El backdoor permite la carga/descarga de archivos, ejecución de comandos de shell y actualizaciones de configuración a través de comandos del servidor de control, comunicándose de manera sigilosa mediante sockets envueltos en RC4.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/new-spectralblur-macos-backdoor-linked-to-north-korea/

Resurgimiento del Malware Qbot en Campañas de FakeUpdates

El malware Qbot, conocido por sus capacidades avanzadas, como keylogging y robo de credenciales, ha vuelto a aparecer en campañas de FakeUpdates. Los atacantes aprovechan esta amenaza para supervisar actividades de navegación, obteniendo información financiera. A pesar de una caída previa, Qbot resurgió en diciembre de 2023, utilizando FakeUpdate, el cual afecta especialmente al sector educativo. Este evento destaca la necesidad de medidas proactivas de seguridad, como seguridad de endpoints o escrutinio de correos electrónicos. Además, se mencionan vulnerabilidades comunes, como Apache Log4j Remote Code Execution y Zyxel ZyWALL Command Injection.

Prioridad: 2 Urgente.

Ampliar información:

https://gbhackers.com/qbot-malware-via-fakeupdates/

Nuevos Paquetes Maliciosos de PyPI Instalan CoinMiner en Dispositivos Linux

Se han identificado tres paquetes maliciosos en PyPI que instalan CoinMiner en dispositivos Linux, afectando el rendimiento. Provenientes de la cuenta "sastra", estos paquetes ocultan su carga útil en una URL remota, dificultando la detección. Su ejecución en varias fases incluye la descarga de un archivo de configuración y el ejecutable CoinMiner, que persiste en el sistema. Las modificaciones se registran en ~/.bashrc, asegurando la reactivación del malware en cada sesión de Bash.

Prioridad: 3 Importante.

Ampliar información:

- https://gbhackers.com/3-new-malicious-pypi-packages/

Pikabot: nuevo malware en ataques Black Basta

Un actor de amenazas vinculado a los ataques de ransomware Black Basta, conocido como Water Curupira, ha desplegado un nuevo cargador en una serie de campañas de phishing que preceden a ataques de ransomware. Identificado como Pikabot, este cargador sofisticado comparte similitudes con el notoriamente difícil de eliminar Qakbot y se utiliza para obtener acceso a las redes de organizaciones con el fin de llevar a cabo actividades maliciosas. El actor, previamente inactivo a finales de junio de 2023, ha reanudado recientemente sus actividades, empleando el nuevo cargador en campañas de phishing que buscan engañar a los usuarios a través de tácticas como el "thread-jacking". Este ataque, que utiliza correos electrónicos que parecen formar parte de conversaciones anteriores, ha aumentado desde el último trimestre de 2023, coincidiendo con la desarticulación de Qakbot

Prioridad: 2 Urgente.

Ampliar información:

- https://www.darkreading.com/cyberattacks-data-breaches/pikabot-malware-qakbot-replacement-black-basta-attacks

---

Recomendaciones generales sobre Malware:

- Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
- Utilizar soluciones de seguridad confiables, como antivirus y firewalls, y mantenerlos actualizados.
- Implementar autenticación multifactor en cuentas y sistemas para agregar una capa adicional de seguridad.
- Educar a los usuarios sobre la importancia de no hacer clic en enlaces o adjuntos sospechosos en correos electrónicos o mensajes.
- Realizar copias de seguridad regulares de los datos importantes y guardarlas en un lugar seguro y fuera de línea.
- Evitar descargar software de fuentes no confiables y solo utilizar tiendas oficiales para obtener aplicaciones.

- Establecer políticas de contraseñas sólidas y cambiarlas regularmente.
- Limitar los privilegios de acceso para los usuarios y las cuentas, y solo otorgar los permisos necesarios.
- Monitorear de cerca la actividad de red y utilizar herramientas de detección de intrusiones.

NOTICIAS DE CIBERSEGURIDAD

Amenaza de ransomware de hackers turcos contra servidores Microsoft SQL en América y Europa

Securonix ha informado sobre una campaña de ransomware, llamada RE#TURGENCE, llevada a cabo por actores turcos motivados financieramente. Estos atacan bases de datos de Microsoft SQL Server en organizaciones de EE. UU., Europa y América Latina. El grupo utiliza fuerza bruta para acceder a las credenciales administrativas, desencadenando así infecciones de ransomware, especialmente Mimic. El informe sugiere que al menos un atacante podría estar ubicado en Turquía, según la lengua turca utilizada en la nota de rescate.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/turkish-hackers-target-microsoft-sql-servers-in-americas-europe/

Ataques de push bombing en Métodos de Autenticación Múltiple (MFA): estrategias y defensas

El push bombing, un ataque dirigido de fatiga en la autenticación multifactor (MFA), ha ganado popularidad entre los ciberdelincuentes al aprovechar contraseñas robadas o filtradas. Este método explota la repetición de la aprobación de mensajes push por parte de los usuarios, induciéndolos a hacer clic por error. Aunque la concienciación del usuario es esencial, las técnicas adaptativas de

MFA y las medidas resistentes al phishing se han convertido en defensas clave contra estos ataques, buscando no solo educar al usuario, sino también fortalecer las tecnologías subyacentes para prevenir intrusiones exitosas.

Prioridad: 2 Urgente.

Ampliar información:

- https://blog.segu-info.com.ar/2024/01/ataques-de-push-bombing-en-metodos-de.html

---

OpenAI Lanza la 'GPT Store': interactúa con millones de versiones modificadas de ChatGPT

OpenAI ha cumplido su anuncio y lanzó la 'GPT Store', una tienda en línea que ofrece millones de versiones modificadas de ChatGPT. Esta nueva funcionalidad, reservada actualmente para usuarios de ChatGPT Plus, Enterprise y Teams, permite a los usuarios explorar y probar versiones adaptadas del popular chatbot. Desde su lanzamiento, se han creado más de tres millones de estas versiones modificadas, desarrolladas tanto por usuarios independientes como por colaboradores oficiales. Además, OpenAI planea permitir a los creadores obtener ingresos económicos mediante un programa que se espera lanzar en el primer trimestre del año. Esta iniciativa marca un paso significativo en la expansión de las capacidades de ChatGPT y su impacto en la industria tecnológica.

Prioridad: 3 Importante.

Ampliar información:

- https://www.genbeta.com/actualidad/chatgpt-se-expande-lanzamiento-gpt-store-tienda-versiones-modificadas-su-ia-asi-funciona

---