GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4923

BOLETIN 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	2	
MALWARE	1	2	2
NOTICIAS DE CIBERSEGURIDAD	1	1	2

VULNERABILIDADES

Vulnerabilidad Reciente en Apache Struts 2 Bajo la Lupa de los Atacantes

Los atacantes están intentando explotar una vulnerabilidad crítica de ejecución remota de código (RCE) recientemente revelada en Apache Struts 2. La falla, identificada como CVE-2023-50164, fue divulgada la semana pasada, y los actores de amenazas ya están sondeando instancias de Apache Struts 2 accesibles por Internet. La vulnerabilidad, con una puntuación de gravedad crítica de 9.8 en el Sistema de Puntuación de Vulnerabilidades Comunes (CVSS), reside en la lógica de carga de archivos de Struts y podría permitir la travesía de rutas, lo que habilita a un atacante a cargar un archivo malicioso y lograr una ejecución remota de código. Se insta a los usuarios de Struts a aplicar los parches proporcionados por Apache de inmediato.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/recent-apache-struts-2-vulnerability-in-attacker-crosshairs/

Servidores pfSense Vulnerables a Ataques de Ejecución Remota de Código

Investigadores descubrieron dos vulnerabilidades en pfSense CE relacionadas con Cross-Site Scripting (XSS) e Inyección de Comandos que permiten a un atacante ejecutar comandos arbitrarios en un dispositivo pfSense. Estas vulnerabilidades podrían ser explotadas para controlar el firewall, monitorear el tráfico en la red local y dirigirse a servicios dentro de la red. Las versiones afectadas son pfSense CE 2.7.0 y anteriores, y pfSense Plus 23.05.1 y anteriores. Se recomienda aplicar el parche disponible en pfSense CE 2.7.1 y pfSense Plus 23.09 para corregir estas vulnerabilidades críticas.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/1450-pfsense-servers-rce-attack/

Vulnerabilidad Crítica en Sophos Firewall Permite Ejecución Remota de Código

Se ha descubierto una vulnerabilidad crítica en el Portal de Usuario y Webadmin de Sophos Firewall que permite a los atacantes ejecutar código malicioso de forma remota. Los dispositivos vulnerables que ejecutan versiones antiguas de firmware han llegado al final de su vida útil, sin recibir actualizaciones ni soporte. Sophos ha lanzado un parche para versiones afectadas, instándoles a tomar medidas de seguridad, como deshabilitar el acceso WAN a User Portal y Webadmin, y utilizar VPN o Sophos Central para acceso remoto.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/sophos-firewall-code-injection-flaw/

Apple lanza iOS 17.2 con Parches de Seguridad Urgentes

Apple ha lanzado iOS 17.2 y iPadOS 17.2 con correcciones para al menos 11 vulnerabilidades de seguridad, algunas de las cuales podrían llevar a la ejecución de código arbitrario o a la fuga del sandbox de la aplicación. Las vulnerabilidades abordadas incluyen problemas de corrupción de memoria en ImageIO, ejecución de código en el motor de renderizado WebKit y problemas de seguridad en la memoria. Apple también ha lanzado iOS 16.7.3 y iPadOS 16.7.3 para dispositivos que ejecutan versiones más antiguas del sistema operativo, que incluyen correcciones para problemas previamente documentados en WebKit.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/apple-ships-ios-17-2-with-urgent-security-patches/

Dell Insta a Clientes a Parchear Vulnerabilidades en Productos PowerProtect

Dell ha notificado a los clientes de sus productos PowerProtect sobre ocho vulnerabilidades, varias de ellas con una calificación de 'alta severidad', instándoles a instalar parches. Las vulnerabilidades afectan a varios productos, incluidos los aparatos PowerProtect Data Domain (DD) y PowerProtect DP, y abarcan problemas como scripting entre sitios (XSS), inyección de comandos del sistema operativo y control de acceso inadecuado. La más seria es una vulnerabilidad XSS basada en DOM con un puntaje CVSS de 8.8. Dell recomienda revisar su asesoría de seguridad y aplicar los parches de inmediato para mitigar posibles riesgos de explotación.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/dell-urges-customers-to-patch-vulnerabilities-in-powerprotect-products/

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

Nuevo Malware NKAbuse Utiliza Tecnología Blockchain para Ataques DDoS

Un malware recientemente descubierto, denominado NKAbuse, está utilizando la tecnología de cadena de bloques NKN (New Kind of Network) como canal de comunicación para llevar a cabo ataques de denegación de servicio distribuidos (DDoS). La amenaza utiliza NKN para el intercambio de datos entre pares, actuando como un implante potente con capacidades de inundación y puerta

trasera. Desarrollado en el lenguaje de programación Go, se dirige principalmente a sistemas Linux, incluidos dispositivos IoT en Colombia, México y Vietnam. La utilización de la tecnología blockchain asegura la fiabilidad y el anonimato, permitiendo que la botnet asociada se expanda de manera constante sin un controlador central identificable.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/12/new-nkabuse-malware-exploits-nkn.html?&web_view=true

---

PikaBot: Nuevo Malware Distribuido a Través de Anuncios de Búsqueda Maliciosos

El malware PikaBot, recientemente descubierto, se está distribuyendo mediante anuncios maliciosos en motores de búsqueda. Este enfoque aprovecha la tendencia creciente de utilizar malvertising para dirigirse a empresas. TA577, el grupo de amenazas asociado a PikaBot, previamente lo distribuía a través de malspam. Este malware, conocido por su capacidad para funcionar como implante y realizar ataques DDoS utilizando la tecnología blockchain NKN, ahora ha adoptado el malvertising como un método de distribución efectivo.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.malwarebytes.com/blog/threat-intelligence/2023/12/pikabot-distributed-via-malicious-ads?&web_view=true

---

116 Paquetes de Malware en PyPI Infectan Sistemas Windows y Linux

Descubiertos 116 paquetes maliciosos en el repositorio PyPI, diseñados para infectar sistemas Windows y Linux. Descargados más de 10,000 veces desde mayo de 2023, estos paquetes contienen backdoors que permiten ejecución remota de comandos, exfiltración de datos y capturas de

pantalla. Este hallazgo se suma a la preocupante tendencia de paquetes Python comprometidos en ataques a la cadena de suministro. Se insta a los desarrolladores a revisar cuidadosamente el código antes de la instalación para prevenir estas amenazas.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/12/116-malware-packages-found-on-pypi.html

---

Nuevo Botnet KV Apunta a Dispositivos de Cisco, DrayTek y Fortinet para Ataques Sigilosos

Un nuevo botnet, conocido como KV, está utilizando firewalls y routers de Cisco, DrayTek, Fortinet y NETGEAR para realizar transferencias de datos de manera encubierta. Este botnet, vinculado a actores de amenazas avanzadas como Volt Typhoon en China, se ha activado desde febrero de 2022. Infecta dispositivos en el borde de las redes y se sospecha que está siendo utilizado para operaciones manuales contra objetivos de alto perfil. Microsoft ha destacado que el botnet busca ocultarse en la actividad normal de la red al enrutar el tráfico a través de equipos de red comprometidos.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2023/12/new-kv-botnet-targeting-cisco-draytek.html

---

Hackers Espían iPhones con Teclados Maliciosos

Se ha descubierto un nuevo método de keylogging que utiliza aplicaciones de teclado maliciosas para afectar a iPhones, burlando las medidas de seguridad de Apple. Los hackers pueden robar contraseñas y datos sensibles utilizando esta técnica, que explota una función existente en el

sistema iOS. Esta amenaza es compatible con todos los modelos de iPhone y destaca por su sencillez de explotación. La revisión laxa de las aplicaciones TestFlight contribuye a su viabilidad. Se recomienda a los usuarios eliminar cualquier teclado no reconocido para evitar el riesgo.

Prioridad: 3 Importante.

Ampliar información:

- https://gbhackers.com/hackers-spy-iphone-users/#google_vignette

---

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

Zoom Lanza Sistema de Puntuación de Impacto de Vulnerabilidades de Código Abierto

Zoom ha presentado un nuevo sistema de puntuación de impacto de vulnerabilidades de código abierto llamado Vulnerability Impact Scoring System (VISS). Este sistema, que ha sido desarrollado durante el último año, ofrece una interfaz de usuario basada en web y algoritmos para ayudar a las organizaciones a evaluar y priorizar vulnerabilidades en función de su explotación real, en lugar de su impacto teórico. VISS pretende complementar el ampliamente utilizado Common Vulnerability Scoring System (CVSS) y ha sido probado dentro del programa de recompensas por errores de Zoom desde marzo. Zoom afirma que el uso de VISS ha llevado a un aumento en los informes que describen vulnerabilidades críticas y de alta gravedad, con investigadores invirtiendo más tiempo y energía para demostrar la practicidad de sus exploits.

Prioridad: 3 Importante.

Ampliar información:

- https://www.securityweek.com/zoom-unveils-open-source-vulnerability-impact-scoring-system/

MongoDB Confirma Hackeo: Datos de Clientes en Riesgo

La compañía de software de bases de datos, MongoDB, ha revelado un hackeo en sus sistemas corporativos, advirtiendo que se han comprometido metadatos y detalles de contacto de las cuentas de los clientes. Aunque aseguran no tener conocimiento de una exposición de los datos almacenados en MongoDB Atlas, su producto principal, instan a los clientes a mantenerse alerta ante posibles ataques de ingeniería social y phishing, recomendando medidas como la activación de la autenticación multifactor y la rotación regular de contraseñas.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/mongodb-confirms-hack-says-customer-data-stolen/

Quishing: Nueva Técnica Sofisticada de Phishing con Códigos QR

Los ciberataques de phishing han evolucionado con la aparición del "quishing", una táctica que utiliza códigos QR maliciosos. Trellix detectó más de 60,000 ejemplos en un trimestre, apuntando a usuarios con tácticas como phishing postal y ataques de malware. Se advierte a los usuarios que sean cautelosos al escanear códigos QR, ya que podrían redirigir a sitios web fraudulentos que buscan robar información sensible. La popularidad creciente de los códigos QR y la disponibilidad de plataformas de "phishing como servicio" contribuyen a la propagación de esta amenaza.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/quishing-sophisticated-phishing-attacks/

MITRE Presenta Modelo de Amenazas EMB3D para Dispositivos en Infraestructuras Críticas

MITRE ha colaborado con Red Balloon Security, Narf Industries y Niyo 'Little Thunder' Pearson de ONE Gas para desarrollar EMB3D, un nuevo modelo de amenazas destinado a dispositivos integrados en infraestructuras críticas. EMB3D busca proporcionar un marco colaborativo que permita una comprensión común de las amenazas y su mitigación. Dirigido a fabricantes, vendedores y propietarios de activos, el modelo se centra en dispositivos integrados, brindando una base de conocimientos de amenazas y mitigaciones técnicas. El lanzamiento oficial está programado para principios de 2024 después de un período de revisión previa.

Prioridad: 3 Importante.

Ampliar información:

- https://www.securityweek.com/mitre-unveils-emb3d-threat-model-for-embedded-devices-used-in-critical-infrastructure/
