GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3523

En alianza con

TD SYNNEX FORTINET

BOLETIN DE CIBERINTELIGENCIA DE AMENAZAS

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	5	3	
MALWARE	2	3	
NOTICIAS DE CIBERSEGURIDAD	5	4	1

VULNERABILIDADES

Notepad++ 8.5.7 Corrige Vulnerabilidades Críticas de Ejecución

Notepad++ versión 8.5.7, corrige múltiples vulnerabilidades de desbordamiento de búfer, algunas de las cuales podrían permitir la ejecución de código malicioso si los usuarios abren archivos manipulados. Estas vulnerabilidades fueron reportadas por un investigador de seguridad de GitHub y se ha publicado evidencia de su explotación, por lo que es esencial que los usuarios actualicen el programa de inmediato. La actualización soluciona estas vulnerabilidades y otros errores.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/notepad-plus-plus-857-released-with-fixes-for-four-security-vulnerabilities/?&web_view=true

Cisco encuentra 8 vulnerabilidades en la plataforma de datos de IoT industrial de la OEA

Cisco ha advertido sobre múltiples vulnerabilidades en la plataforma Open Automation Software (OAS), utilizada en entornos industriales y empresariales. Estas vulnerabilidades incluyen fallos de elusión de autenticación que podrían permitir a un atacante crear nuevos usuarios y acceder a sistemas subyacentes. Se recomienda actualizar a la versión más reciente de OAS para resolver estos problemas de seguridad.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/cisco-finds-8-vulnerabilities-in-oas-industrial-iot-data-platform/?web_view=true

---

Vulnerabilidades Críticas Apache Superset permiten la Ejecución de Código Remoto

Un par de vulnerabilidades de seguridad en Apache Superset podrían ser explotadas por un atacante para lograr la ejecución de código remoto en sistemas vulnerables. Superset es una plataforma de visualización y exploración de datos de código abierto escrita en Python. La versión 2.1.1 abordó dos vulnerabilidades, identificadas como CVE-2023-39265 y CVE-2023-37941, que podrían permitir el control de la base de datos de metadatos de Superset. Estas vulnerabilidades podrían llevar a la obtención de credenciales y la ejecución de código remoto. Se recomienda actualizar a la última versión de Superset para corregir estos problemas de seguridad.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/multiple-splunk-enterprise-flaws/

Google abordo un día cero activamente explotado en Android

Google ha lanzado las actualizaciones de seguridad de Android de septiembre de 2023 para solucionar varias vulnerabilidades, incluyendo una vulnerabilidad zero-day en el componente Framework que permitiría a un atacante aumentar sus privilegios sin necesidad de interacción del usuario. También se han solucionado tres vulnerabilidades críticas de ejecución de código remoto en el componente System y una vulnerabilidad crítica en componentes cerrados de Qualcomm. Se recomienda a los usuarios actualizar sus dispositivos Android cuanto antes para protegerse contra estas amenazas.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/150440/hacking/september-2023-android-security-updates-0day.html?web_view=true

---

Investigadores descubren una vulnerabilidad crítica en PHP Fusión

Se ha encontrado una grave vulnerabilidad en PHP Fusion, un sistema de gestión de contenidos, que permite a los atacantes ejecutar código de forma remota al cargar un archivo malicioso en el sistema. También se descubrió una vulnerabilidad moderada que permite a los atacantes leer y escribir archivos en el sistema afectado. Estas vulnerabilidades afectan a varias versiones de PHP Fusion y aún no se han lanzado parches debido a la falta de respuesta de los desarrolladores.

Prioridad: 1 Crítico.

Ampliar información:

https://www.darkreading.com/application-security/researchers-discover-critical-vulnerability-in-phpfusion-cms?&web_view=true

---

Vulnerabilidad SAML de Mend.io expuesta

Mend.io, un proveedor de soluciones de seguridad de aplicaciones, ha resuelto recientemente una vulnerabilidad de seguridad en su sistema de inicio de sesión SAML. La falla podría haber permitido a usuarios maliciosos acceder a los datos de otros clientes dentro del mismo entorno SaaS al adivinar direcciones de correo electrónico válidas. Aunque no se ha informado de ninguna explotación activa, Mend.io solucionó rápidamente el problema. Se aconseja a los clientes que revisen los registros en busca de posibles abusos.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.infosecurity-magazine.com/news/mendios-saml-vulnerability-exposed/?&web_view=true

---

Múltiples vulnerabilidades de ArubaOS permiten a los atacantes ejecutar código arbitrario

Se han encontrado vulnerabilidades críticas en los controladores y gateways de las series Aruba 9200 y 9000 que ejecutan ArubaOS. Estas vulnerabilidades podrían permitir a un atacante ejecutar código arbitrario y eludir las medidas de seguridad. Aruba ha lanzado parches para abordar estas vulnerabilidades, y se recomienda a los usuarios actualizar a las versiones corregidas para proteger sus sistemas.

Prioridad: 1 Critico

Ampliar información:

- https://gbhackers.com/multiple-arubaos-vulnerabilities/

Una falla en la implementación de SSO en Cisco Broadworks permitió a atacantes falsificar credenciales.

Se ha identificado una vulnerabilidad crítica en las plataformas Cisco BroadWorks Application Delivery y Cisco BroadWorks Xtended Services Platform. Esta vulnerabilidad podría ser aprovechada por un atacante remoto y no autenticado para falsificar credenciales y acceder a un sistema vulnerable. Cisco ha lanzado actualizaciones de software para abordar este problema, y no existen soluciones alternativas disponibles. La vulnerabilidad se debe a un error en la implementación de la función de inicio de sesión único (SSO).

Prioridad: 1 Critico.

Ampliar información:

https://gbhackers.com/cisco-broadworks-flaw/

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

La variante del botnet Mirai 'Pandora' secuestra televisores Android para realizar ciberataques

Se ha detectado una variante de la botnet Mirai llamada Pandora que está infiltrando dispositivos basados en Android como televisores, utilizándolos para llevar a cabo ataques DDoS. Estas infiltraciones suelen ocurrir a través de actualizaciones de firmware maliciosas o la instalación de aplicaciones para ver contenido pirateado. La botnet Pandora es capaz de infectar estos dispositivos y utilizarlos en ataques, especialmente aquellos que tienen procesadores de cuatro núcleos de Allwinner y Amlogic. Para protegerse contra estas amenazas, se recomienda a los usuarios mantener sus dispositivos actualizados y descargar software solo desde fuentes de confianza.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/09/mirai-botnet-variant-pandora-hijacks.html?&web_view=true/

El nuevo malware BlueShell ataca a Windows, Linux y Mac

El malware BlueShell está en aumento afectando a Windows, Mac y Linux. El grupo Dalbit de China lo usa para atacar servidores vulnerables y robar datos. Además, se encontró una variante personalizada. Se han observado otros ataques en sistemas MinIO, Linux y Mac. Para protegerse, se recomienda actualizar sistemas, usar detección de intrusiones y concienciar a los usuarios sobre phishing.

Prioridad: 2 Urgente.

Ampliar información:

- https://cyware.com/news/new-blueshell-malware-attacks-windows-linux-and-mac-d3c9445e/?web_view=true

---

Campaña de Malware Amenaza a Ecosistemas Python, JavaScript y Ruby

Phylum ha descubierto una campaña de malware que afecta a los ecosistemas de Python, JavaScript y Ruby. En esta campaña, se publican paquetes maliciosos que recopilan información de máquinas macOS y la envían a un servidor controlado por un atacante. Phylum ha informado a los respectivos ecosistemas para eliminar estos paquetes y recomienda a los desarrolladores utilizar soluciones automatizadas para protegerse contra el malware en registros de paquetes de código abierto.

Prioridad: 2 Urgente.

Ampliar información:

- https://blog.phylum.io/malware-campaign-targets-npm-pypi-and-rubygems-developers/?&web_view=true

---

El malware DreamBus explota servidores RocketMQ sin parches

Los actores de amenazas están explotando una vulnerabilidad de ejecución remota de código conocida en servidores RocketMQ para infectar dispositivos con malware DreamBus. La vulnerabilidad CVE-2023-33246 fue descubierta en mayo de 2023 y se calificó como crítica, con una puntuación de 9.8. Afecta a RocketMQ versión 5.1.0 y anteriores, lo que permite a los atacantes ejecutar código de forma remota en ciertas condiciones. Para prevenir esta amenaza, se recomienda a los usuarios de RocketMQ actualizar a la versión 5.1.1 o posterior y utilizar soluciones de gestión de parches automatizadas para mantener sus sistemas actualizados.

Prioridad: 1 CrÍtico.

Ampliar información:

- https://heimdalsecurity.com/blog/dreambus-malware-rocketmq/

Ransomware Monti publica nueva versión para Linux

El grupo detrás del ransomware Monti ha lanzado una nueva versión dirigida a sectores gubernamentales y legales. A diferencia de las versiones anteriores, esta variante utiliza un cifrado diferente y ha realizado cambios para evadir la detección. Monti emplea AES-256-CTR y ajusta su cifrado según el tamaño de los archivos, dificultando su detección y mitigación. Los expertos en seguridad advierten sobre la importancia de contar con medidas sólidas de seguridad para protegerse contra este ransomware en constante evolución.

Prioridad: 1 Critico.

Ampliar información:

- https://blog.segu-info.com.ar/2023/09/ransomware-monti-publica-nueva-version.html

---

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

Apple Lanza Actualizaciones de Emergencia tras Ataques de Spyware Pegasus

Apple ha lanzado actualizaciones de seguridad de emergencia para iOS, iPadOS, macOS y watchOS debido a dos vulnerabilidades zero-day que se han aprovechado para distribuir el spyware Pegasus de NSO Group. Estas vulnerabilidades permitían la ejecución de código malicioso. Una de ellas se encontraba en la aplicación Wallet, y la otra en el componente Image I/O. Citizen Lab informó que estas vulnerabilidades se utilizaron en ataques a iPhones completamente actualizados a través de iMessage, sin necesidad de interacción por parte del usuario. Estas actualizaciones son parte de los esfuerzos continuos de Apple para abordar las amenazas de seguridad.

Prioridad: 1 Critico.

Ampliar información:

- https://thehackernews.com/2023/09/apple-rushes-to-patch-zero-day-flaws.html?&web_view=true

---

APT34 Utiliza Backdoor SideTwist en Nuevo Ataque de Phishing: Alerta por Campaña de Agent Tesla que Explota Vulnerabilidad Antigua de Office

El grupo de amenaza iraní APT34 está detrás de un nuevo ataque de phishing que utiliza el backdoor SideTwist. APT34 es conocido por su sofisticación y capacidad para crear herramientas avanzadas. Además, se ha descubierto una campaña de phishing que distribuye una variante de Agent Tesla

explotando una antigua vulnerabilidad de Office. Esta vulnerabilidad, CVE-2017-11882, sigue siendo utilizada por numerosos actores maliciosos. Mantener el software actualizado y ser cauteloso ante el phishing es esencial para la seguridad en línea.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/09/alert-phishing-campaigns-deliver-new.html?&web_view=true

---

Explotaciones malvadas de MinIO: un nuevo vector de ataque para violar las redes corporativas

Security Joes ha detectado un actor desconocido aprovechando vulnerabilidades en el sistema de almacenamiento de objetos MinIO para ejecutar código en servidores vulnerables. Se han encontrado más de 50,000 instalaciones de MinIO vulnerables en línea. Se insta a los administradores a verificar la autenticidad de las fuentes al instalar software de código abierto y aplicar las actualizaciones de seguridad disponibles.

Prioridad: 1 Critico.

Ampliar información:

- https://cyware.com/news/evil-minio-exploits-a-new-attack-vector-to-breach-corporate-networks-ed65b661/?web_view=true

---

Meta elimina miles de cuentas involucradas en operaciones de desinformación de China y Rusia

Meta ha desmantelado dos operaciones de influencia encubierta de China y Rusia, bloqueando miles de cuentas y páginas. La operación rusa, Doppelganger, difundió noticias falsas sobre Ucrania

y usó typosquatting en nombres de dominio. También se bloquearon miles de dominios web maliciosos.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2023/09/meta-takes-down-thousands-of-accounts.html?&web_view=true

---

Dispositivos Flipper Zero Pueden Realizar Ataques de Denegación de Servicio en iPhones y Vulnerar Llaves de Automóviles y Tarjetas RFID

Ciertos dispositivos Flipper Zero pueden realizar ataques de Denegación de Servicio (DoS) en iPhones al inundarlos con ventanas emergentes. También pueden atacar llaves de automóviles y tarjetas RFID. El investigador sugiere que Apple implemente medidas de seguridad para reducir el riesgo. En resumen, los Flipper Zero pueden causar interrupciones en iPhones y otros dispositivos cercanos.

Prioridad: 1 Critico.

Ampliar información:

- https://gbhackers.com/flipper-device-iphone/

Las extensiones de Chrome pueden robar contraseñas en texto plano de sitios web

Un equipo de investigadores ha demostrado cómo las extensiones de Chrome pueden robar contraseñas en texto plano de sitios web debido a un acceso ilimitado a los datos del sitio. A pesar de las medidas de seguridad, este problema afecta al 12.5% de las extensiones en la Chrome Web Store, incluidas algunas populares. Grandes empresas como Amazon, Google y Facebook también

son vulnerables. La investigación destaca la necesidad de proteger los datos sensibles en línea y resalta la importancia de utilizar contraseñas seguras.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/chrome-extensions-can-steal-plaintext-passwords-from-websites/

Protección de servidores Microsoft IIS contra ataques de malware

Lazarus, un grupo ciberdelincuente notorio, está atacando activamente servidores vulnerables de Microsoft Internet Information Services (IIS). Explotan vulnerabilidades para insertar malware y distribuir código malicioso. Proteger sus servidores IIS implica una gestión efectiva de parches, minimizar los privilegios de cuentas de servicio, analizar registros de red y servidores, e implementar pruebas de seguridad continuas en aplicaciones web para detectar vulnerabilidades de manera oportuna. Este enfoque integral garantiza que los servidores permanezcan seguros contra amenazas como Lazarus.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/09/protecting-your-microsoft-iis-servers.html

---

Microsoft desactivará TLS 1.0 y 1.1 en Windows, SQL Server, Office, etc

Microsoft eliminará los protocolos inseguros TLS 1.0 y 1.1 en futuras versiones de Windows. Recomienda que los desarrolladores adopten TLS 1.3 para mejorar la seguridad. Esta transición afectará principalmente a nuevas versiones de Windows y podría romper algunas aplicaciones más antiguas. Microsoft advierte que podría eliminar por completo el soporte para TLS 1.0 y 1.1 en el futuro.

Prioridad: 1 Crítico.

Ampliar información:

- https://blog.segu-info.com.ar/2023/09/microsoft-desactivara-tls-10-y-11-en.html

---

Alerta de Seguridad: Spyware Peligroso se Hace Pasar por Modificaciones de Telegram en Google Play: Riesgos para Usuarios Empresariales

Se ha descubierto spyware peligroso que se hace pasar por modificaciones legítimas de Telegram en Google Play. Estas aplicaciones maliciosas han sido descargadas decenas de miles de veces y presentan graves riesgos para los usuarios empresariales. El spyware monitorea constantemente la actividad de Telegram y extrae información. Las empresas deben advertir a los empleados sobre los riesgos de usar aplicaciones de terceros y solo utilizar aplicaciones oficiales y de confianza. También deben prestar atención a las reseñas de los usuarios y la información del desarrollador antes de descargar aplicaciones.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.darkreading.com/attacks-breaches/evil-telegram-spyware-campaign-infects-60k-mobile-users

---

W3LL Gang compromete miles de cuentas de Microsoft 365

El grupo de ciberdelincuentes W3LL ha comprometido más de 8,000 cuentas de Microsoft 365 en 10 meses. Usan herramientas de phishing y han creado un mercado subterráneo para otros ciberdelincuentes. Su kit de phishing, llamado W3LL Panel, puede evadir la autenticación de múltiples factores. Las víctimas son empresas de varios sectores. W3LL ofrece soporte y tutoriales para ciberdelincuentes sin experiencia técnica. Estos ataques pueden resultar en pérdidas financieras, filtración de datos y daño a la reputación. Las organizaciones deben reforzar su ciberseguridad y capacitar a los empleados.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.darkreading.com/endpoint/w3ll-gang-compromises-thousands-of-microsoft-365-accounts

---