GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3723

BOLETÍN 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	5	
MALWARE	2	2	2
NOTICIAS DE CIBERSEGURIDAD	2	1	1
SECTOR FINANCIERO	1		

VULNERABILIDADES

GitLab parchea una vulnerabilidad crítica de ejecución de canalización

GitLab ha emitido una actualización de seguridad para abordar una vulnerabilidad crítica, CVE-2023-5009, que permite a un atacante ejecutar canalizaciones como otro usuario. Esta vulnerabilidad afecta a varias versiones de GitLab CE y EE. Se recomienda encarecidamente a los usuarios actualizar a las versiones 16.3.4 y 16.2.7 para resolver este problema y proteger sus sistemas. En versiones anteriores a la 16.2, la vulnerabilidad solo es relevante si ciertas funciones están habilitadas simultáneamente.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/gitlab-patches-critical-pipeline-execution-vulnerability/

Drupal publica un aviso de seguridad para abordar vulnerabilidad en Drupal Core

Drupal ha emitido un aviso de seguridad para abordar una vulnerabilidad que afecta a varias versiones de Drupal. Un actor cibernético malicioso podría aprovechar esta vulnerabilidad para tomar el control de un sistema afectado. Se alienta a los usuarios y administradores a revisar el aviso de seguridad de Drupal, denominado SA-CORE-2023-006, para obtener más información y aplicar las actualizaciones necesarias.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.cisa.gov/news-events/alerts/2023/09/21/drupal-releases-security-advisory-address-vulnerability-drupal-core

---

Vulnerabilidades en MOVEit Transfer Service Pack

Se han encontrado tres vulnerabilidades en MOVEit Transfer Service Pack, incluyendo dos inyecciones SQL y un problema de seguridad Cross-Site Scripted (XSS). Las vulnerabilidades afectan a varias versiones del software y podrían dar lugar a accesos no autorizados y ejecución de código malicioso. Se recomienda a los usuarios actualizar a la última versión para resolver estas vulnerabilidades. Organizaciones como Shell, BBC y otras fueron afectadas por estas amenazas.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/moveit-transfer-sql-injection/

Vulnerabilidad en Trend Micro Apex One y Otras Soluciones.

Se ha descubierto una vulnerabilidad en Trend Micro Apex One y otras soluciones de seguridad que podría permitir a los atacantes ejecutar código malicioso en sistemas vulnerables. La amenaza ha sido detectada en el mundo real y se aconseja a los usuarios actualizar sus productos a las versiones más recientes para protegerse. La vulnerabilidad, identificada como CVE-2023-41179, tiene un puntaje de gravedad de 9.1 (Crítica) y afecta a ciertas versiones de los productos mencionados. Se requiere acceso a la consola administrativa en la máquina objetivo para explotar esta vulnerabilidad. Las versiones corregidas se detallan en la información proporcionada.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/trend-micro-zero-day-vulnerability/

Vulnerabilidades de Cross-Site Scripting (XSS) en Azure HDInsight

Se han identificado múltiples vulnerabilidades de Cross-Site Scripting (XSS) en Azure HDInsight relacionadas con Stored XSS (XSS almacenado) y Reflected XSS (XSS reflejado). Estas vulnerabilidades afectaron a varios productos, incluyendo Azure Apache Oozie, Apache Ambari, Jupyter Notebooks, Apache Hadoop y Apache Hive 2. Microsoft ha solucionado estas vulnerabilidades en su actualización de seguridad de agosto. Se descubrieron 6 vulnerabilidades de Stored XSS y 2 de Reflected XSS, con impactos y severidades variadas. Se recomienda a los usuarios de estos productos que actualicen a la última versión para prevenir la explotación de estas vulnerabilidades.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/xss-vulnerabilities-azure-hdinsight/

Vulnerabilidades en Nagios XI: Riesgos Detectados en la Monitorización de Redes

Se han descubierto cuatro vulnerabilidades de seguridad en el software de monitoreo de redes Nagios XI, en versiones anteriores a la 5.11.2. Estas vulnerabilidades podrían permitir a atacantes acceder a datos confidenciales y aumentar sus privilegios en el sistema. Las vulnerabilidades incluyen inyección SQL y un problema de scripting entre sitios (XSS). Se recomienda encarecidamente a los usuarios de Nagios XI que actualicen a la última versión para proteger sus sistemas de posibles amenazas.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/09/critical-security-flaws-exposed-in.html

---

Vulnerabilidad de Ejecución Remota de Código en Firewalls Juniper

Investigadores de VulnCheck han descubierto una vulnerabilidad de ejecución remota de código, denominada CVE-2023-36845, que afecta a cerca de 12,000 dispositivos de firewall Juniper expuestos en Internet. Esta vulnerabilidad puede ser explotada por atacantes no autenticados y remotos para ejecutar código arbitrario en los firewalls Juniper sin necesidad de crear archivos en el sistema. Aunque Juniper Networks lanzó un parche para solucionar esta y otras vulnerabilidades relacionadas el mes pasado, es esencial que los usuarios apliquen los parches correspondientes para mitigar posibles amenazas.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/09/over-12000-juniper-firewalls-found.html

---

Múltiples Vulnerabilidades de Seguridad en la Aplicación Nessus

Se han identificado varias vulnerabilidades de seguridad en la aplicación Nessus, incluyendo una vulnerabilidad de devolución de contraseña, una vulnerabilidad de escritura arbitraria de archivos y una vulnerabilidad de autorización incorrecta. Estas vulnerabilidades podrían permitir a atacantes remotos descubrir credenciales SMTP almacenadas, sobrescribir archivos arbitrarios y ver una lista de todos los usuarios en la aplicación. Tenable ha lanzado Nessus 10.5.5 para abordar estos problemas, y se recomienda a los usuarios que actualicen a la última versión por razones de seguridad.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.tenable.com/security/tns-2023-31

Vulnerabilidades en IBM Spectrum Protect Plus.

Se han descubierto vulnerabilidades en IBM Spectrum Protect Plus que podrían permitir a atacantes locales y remotos obtener privilegios elevados, ejecutar comandos arbitrarios y realizar ataques de denegación de servicio. Estas vulnerabilidades están relacionadas con el kernel de Linux y Python. IBM ha lanzado correcciones para abordar estas vulnerabilidades y se recomienda a los usuarios que actualicen sus sistemas para mitigar los riesgos.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0769/

Vulnerabilidad Crítica en Productos de Trend Micro.

Una vulnerabilidad crítica se ha descubierto en productos de Trend Micro, como Apex One y Worry-Free Business Security. Esto podría permitir a los atacantes ejecutar comandos en sistemas

afectados. Al menos un intento de ataque se ha observado. Se insta a los usuarios a actualizar sus productos a las últimas versiones para protegerse. Trend Micro ha lanzado parches y soluciones para abordar esta amenaza.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0764/

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

Deadglyph, una puerta trasera sofisticada y desconocida

ESET ha descubierto el sofisticado backdoor Deadglyph, usado por el grupo Stealth Falcon para el espionaje en Oriente Medio. Stealth Falcon, activo desde 2012, atacó a activistas y periodistas. Deadglyph emplea una arquitectura única y lenguajes de programación variados para evadir la detección. Recibe comandos dinámicos y puede desinstalarse para evitar ser detectado. El método de entrega sigue siendo desconocido.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/151298/malware/deadglyph-backdoor-middle-east.html

---

El nuevo grupo APT 'Sandman' ataca a las empresas de telecomunicaciones con un raro malware LuaJIT

Un nuevo grupo APT, denominado Sandman, ha sido identificado atacando a proveedores de telecomunicaciones en Europa y Asia en una campaña de ciberespionaje. Utilizan un sofisticado backdoor modular basado en Lua, un lenguaje de programación poco común en el ámbito de las amenazas cibernéticas. El malware LuaDream, empleado por Sandman, tiene la capacidad de extraer información del sistema y el usuario, lo que sugiere una operación de considerable envergadura. Aunque se desconoce la identidad exacta del grupo, su enfoque cauteloso y estratégico dificulta su rastreo. Además, este hallazgo señala un cambio en el paradigma de desarrollo de malware, ya que el uso de LuaJIT en APTs es poco común y generalmente se asocia con actores de alto nivel.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/new-sandman-apt-group-hitting-telcos-with-rare-luajit-malware/

Nueva Variante de Ransomware BlackCat 'Sphynx' Ataca Cuentas de Almacenamiento Azure

Se ha identificado una nueva variante del ransomware BlackCat llamada 'Sphynx', que ha sido mejorada con características adicionales para cifrar cuentas de almacenamiento de Azure. Esta variante de Sphynx se descubrió por primera vez en marzo y ha sido actualizada en varias ocasiones, incluyendo la adición de la herramienta de exfiltración Exmatter. Los actores de amenazas detrás de esta variante han utilizado técnicas avanzadas para acceder a las claves de Azure de los clientes y cifrar múltiples cuentas de almacenamiento.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/blackcat-ransomware/

Campaña de malware en América Latina distribuye troyano bancario BBTok

Una campaña de malware en América Latina está propagando BBTok, un troyano bancario que afecta a usuarios en Brasil y México. Este troyano simula interfaces de más de 40 bancos y engaña a las víctimas para que revelen información sensible. Se entrega a través de correos de phishing. Aunque opera desde 2020, sigue siendo una amenaza activa en la región.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/09/new-variant-of-banking-trojan-bbtok.html

---

Falso PoC de Vulnerabilidad en WinRAR Intenta Propagar Malware RAT

Un actor malicioso publicó un falso "proof-of-concept" (PoC) en GitHub para una vulnerabilidad recientemente revelada en WinRAR con la intención de infectar a usuarios que descargaron el código con malware RAT Venom. Aunque este tipo de falsos PoCs son comunes para atacar a la comunidad de investigación, en este caso se sospecha que los actores maliciosos también están apuntando a otros criminales que podrían estar adoptando las últimas vulnerabilidades en su arsenal. La vulnerabilidad CVE-2023-40477 en WinRAR permitiría la ejecución remota de código y fue corregida en una actualización anterior.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2023/09/beware-fake-exploit-for-winrar.html

---

Operación de Cryptojacking en la Nube de AWS Ataca Servicios Poco Comunes

Una operación de cryptojacking en la nube, denominada AMBERSQUID por la firma de seguridad Sysdig, se ha centrado en servicios inusuales de Amazon Web Services (AWS) como AWS Amplify, AWS Fargate y Amazon SageMaker para minar criptomonedas de manera ilícita. Los atacantes indonesios detrás de esta operación aprovechan imágenes de Docker Hub y abusan de AWS CodeCommit para alojar repositorios Git privados utilizados en varios servicios. AMBERSQUID podría generar pérdidas de más de $10,000 al día si se amplía para atacar todas las regiones de AWS, y hasta ahora ha generado más de $18,300 en ingresos para los atacantes.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2023/09/new-ambersquid-cryptojacking-operation.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

Así es el último phishing 'casi perfecto' a través de Wallapop

Los ciberdelincuentes han ideado un elaborado ataque de phishing a través de Wallapop para robar datos bancarios. Se dirigen a usuarios nuevos y novatos, ganan su confianza, falsifican una transacción y envían correos electrónicos fraudulentos que parecen ser de Wallapop. Aunque algunas personas lograron evitar ser estafadas, se advierte a todos los usuarios que desconfíen de las solicitudes de datos personales o bancarios y verifiquen la autenticidad de los mensajes y sitios web.

Prioridad: 3 Importante.

Ampliar información:

- https://www.pandasecurity.com/es/mediacenter/mobile-news/ultimo-phishing-casi-perfecto-wallapop/

Tácticas de Phishing se Dirigen a Empresas de Mensajería

El phishing se está centrando en empresas de mensajería como Seur y Amazon. Los estafadores envían correos falsos sobre paquetes pendientes para engañar a los usuarios. También se utilizan mensajes de texto y descargas de aplicaciones falsas. Se aconseja verificar si se espera un paquete, revisar el remitente del correo, no proporcionar datos personales y nunca hacer pagos en medio del proceso. El uso de un antivirus actualizado es recomendado.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.pandasecurity.com/es/mediacenter/seguridad/phishing-empresas-logisticas/

Grupo de amenazas Transparent Tribe utiliza aplicaciones Android falsas de YouTube para distribuir el troyano CapraRAT

Transparent Tribe, un grupo de amenazas vinculado a Pakistán, ha estado utilizando aplicaciones Android falsas que parecen ser YouTube para distribuir el troyano de acceso remoto móvil CapraRAT. Estas aplicaciones engañosas se hacen pasar por YouTube y se dirigen a objetivos en la India. Una vez instaladas, estas aplicaciones solicitan permisos intrusivos que les permiten robar datos sensibles y enviarlos a servidores controlados por el grupo. CapraRAT puede realizar llamadas telefónicas y bloquear mensajes SMS entrantes. Se insta a las personas y organizaciones en la India a reforzar sus medidas de seguridad contra esta amenaza.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/09/transparent-tribe-uses-fake-youtube.html

---

Alerta por Malware en Android que Reinicia Teléfonos y Causa Pérdidas de $10 Millones

La policía Singapore ha emitido una advertencia sobre un nuevo malware de Android que, después de ejecutar transacciones no autorizadas en la aplicación bancaria del teléfono, reinicia los dispositivos infectados. Más de 750 personas cayeron en esta estafa en la primera mitad de 2023, perdiendo al menos $10 millones. Las víctimas son atraídas por anuncios falsos en redes sociales, descargan una aplicación maliciosa que roba credenciales bancarias y realiza transacciones fraudulentas antes de reiniciar el dispositivo. Se aconseja a los usuarios precaución al descargar aplicaciones y usar medidas de seguridad como ScamShield y la autenticación de dos factores.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.channelnewsasia.com/singapore/android-malware-scam-factory-reset-phone-police-3785801