GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3223

En alianza con

TD SYNNEX FORTINET

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	3	
MALWARE	2	2	
NOTICIAS DE CIBERSEGURIDAD		2	3

VULNERABILIDADES

Vulnerabilidad en WinRAR de alta gravedad

RARLAB ha lanzado correcciones para una seria vulnerabilidad de seguridad en WinRAR. Esta falla permitía la ejecución arbitraria de código y fue identificada por el investigador "goodbyeselene" de Zero Day Initiative en junio. La actualización de WinRAR a la versión 6.23 soluciona este problema, junto con otra vulnerabilidad de inicio de archivo erróneo. Se recomienda a los usuarios estar atentos a archivos RAR descargados y usar software antivirus para protegerse contra posibles ciberataques.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.scmagazine.com/brief/high-severity-winrar-vulnerability-addressed

16 nuevas fallas de CODESYS SDK exponen los entornos OT a ataques remotos

Se descubrieron 16 vulnerabilidades en el SDK CODESYS V3 que permiten ejecución remota de código y denegación de servicio en sistemas operativos. Estas afectan versiones anteriores a 3.5.19.0 y podrían explotarse para interrumpir operaciones y ejecutar código malicioso en dispositivos de automatización.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/08/15-new-codesys-sdk-flaws-expose-ot.html

Galería de PowerShell propensa a errores tipográficos y otros ataques a la cadena de suministro

El PowerShell Gallery de Microsoft presenta riesgos de seguridad en su cadena de suministro de software debido a su vulnerabilidad al typosquatting y otros ataques. Los investigadores de Aqua Nautilus descubrieron que los atacantes podrían falsificar paquetes maliciosos en el repositorio online al abusar de las políticas de nombres y propietarios. Aunque Microsoft ha intentado solucionar el problema, las protecciones siguen siendo débiles. Se aconseja a las organizaciones utilizar módulos firmados y repositorios confiables para mitigar estos riesgos.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.darkreading.com/application-security/powershell-gallery-prone-to-typosquatting-other-supply-chain-attacks

Vulnerabilidad de ejecución remota de código de Python

Se ha identificado una vulnerabilidad en Python que podría ser explotada por un atacante remoto para ejecutar código de forma remota, revelar información sensible y eludir restricciones de seguridad en el sistema objetivo. Los sistemas afectados incluyen versiones anteriores a Python 3.12, 3.11.4, 3.10.12, 3.9.17, 3.8.17 y 3.7.17.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.hkcert.org/security-bulletin/python-remote-code-execution-vulnerability_20230814

Múltiples vulnerabilidades en productos de Samsung

Se han identificado múltiples vulnerabilidades en productos de Samsung que podrían ser explotadas por un atacante remoto para causar una condición de denegación de servicio, elevar privilegios, ejecutar código de forma remota, manipular datos y revelar información sensible en el sistema objetivo. Los sistemas afectados incluyen versiones de Android 11, 12 y 13.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.hkcert.org/security-bulletin/samsung-products-multiple-vulnerabilities_20230815

Vulnerabilidad en MISP

Se ha identificado una vulnerabilidad en MISP que afecta a versiones anteriores a 2.4.174, permitiendo la inyección remota indirecta de código (XSS). Esto podría ser explotado por un atacante para insertar código malicioso de forma remota. Se recomienda a los usuarios afectados que consulten el boletín de seguridad del proyecto MISP del 17 de agosto de 2023 para obtener los parches y soluciones correspondientes. La referencia CVE de esta vulnerabilidad es CVE-2023-40224.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0662/

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

Malware convirtió miles de PC con Windows y macOS pirateadas en servidores proxy

Ciberdelincuentes están convirtiendo máquinas infectadas con malware en servidores proxy en Windows y macOS, con más de 400,000 nodos de salida de proxy creados. A pesar de la afirmación del servicio proxy de contar con el consentimiento informado del usuario, la evidencia sugiere que se instala malware en sistemas comprometidos de manera silenciosa. Este software proxy, escrito en Go, apunta a ambos sistemas operativos, evadiendo la detección en Windows a través de una firma digital válida.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/08/this-malware-turned-thousands-of-hacked.html

---

QwixxRAT, una nueva RAT de Windows aparece en el panorama de amenazas

QwixxRAT es un nuevo troyano de acceso remoto (RAT) para Windows que se vende en plataformas como Telegram y Discord. Detectado por Uptycs Threat Research en agosto de 2023, el RAT recopila datos sensibles y los envía al bot de Telegram del atacante, permitiéndoles controlar y gestionar el RAT de forma remota. Diseñado meticulosamente para robar información como historiales de navegación y detalles de tarjetas de crédito, el RAT está disponible en diferentes suscripciones y utiliza técnicas de evasión para evitar la detección.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/149525/cyber-crime/qwixxrat-telegramrat.html

La pandilla Monti Ransomware lanzó un nuevo encriptador de Linux

El grupo de ransomware Monti ha vuelto a la acción después de una pausa de dos meses con una nueva variante dirigida a sistemas Linux. Esta versión se ha empleado en ataques contra organizaciones gubernamentales y legales. Aunque se basa en el código filtrado de Conti, esta versión presenta diferencias significativas en su cifrado y comportamiento. El nuevo cifrado utiliza AES-256-CTR en lugar de Salsa20 y verifica las condiciones de cifrado antes de proceder. Además, se observan cambios en el código que indican un intento de evadir la detección, lo que complica la tarea de mitigar los efectos de este ransomware.

Prioridad: 1 Crítico.

Ampliar información:

- https://securityaffairs.com/149539/cyber-crime/monti-ransomware-news-linux-variant.html

XWorm, Remcos RAT evaden EDR para infectar infraestructura crítica

El inyector basado en Rust llamado Freeze[.]rs se ha utilizado para llevar a cabo un ataque de phishing sofisticado que evade las detecciones de EDR. Descubierto por Fortinet's FortiGuard Labs en julio, este ataque emplea un archivo PDF malicioso para comprometer a objetivos en Europa y América del Norte. El ataque culmina en la instalación del malware XWorm, capaz de ejecutar desde ransomware hasta servir como puerta trasera persistente. También se ha identificado la participación de SYK Crypter en la distribución del troyano Remcos. Este enfoque evasivo destaca la importancia de mantener el software actualizado y utilizar herramientas de seguridad avanzadas para defenderse contra los ataques de phishing en constante evolución.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.darkreading.com/ics-ot/xworm-remcos-rat-evade-edrs-infect-critical-infrastructure

---

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

Ataque NoFilter: el método furtivo de escalada de privilegios evita la seguridad de Windows

Se ha descubierto un nuevo método de ataque llamado NoFilter que aprovecha la plataforma de filtrado de Windows (WFP) para lograr una escalada de privilegios en sistemas operativos Windows. Este método permite que un atacante eleve sus privilegios de administrador a "NT AUTHORITY\SYSTEM" de manera sigilosa y evasiva, utilizando una técnica que modifica la duplicación de tokens en el kernel a través de WFP. Esto puede permitir que el atacante inicie procesos con privilegios de sistema sin dejar evidencia, lo que representa un riesgo para la seguridad. El

descubrimiento se presentó en la conferencia de seguridad DEF CON y destaca la importancia de examinar los componentes integrados del sistema operativo en busca de nuevos vectores de ataque.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2023/08/nofilter-attack-sneaky-privilege.html

---

Un grupo hacker ataca 21 sitios web del Gobierno de Japón en protesta contra la liberación de las aguas residuales de Fukushima

Un grupo hacktivista afiliado a Anonymous Italia ha lanzado ciberprotestas contra el gobierno japonés en respuesta a la liberación planificada de aguas residuales tratadas de la Planta Nuclear Fukushima Daini. Bajo el nombre "Tango Down", el grupo ha atacado 21 sitios web gubernamentales y relacionados con la planta. Se ha cuestionado la liberación de las aguas residuales tratadas, ya que podrían dispersar contaminación en el océano y afectar la vida marina. Anonymous Italia también acusa al gobierno japonés de influir en la opinión pública a través de la inteligencia artificial y de sobornar a la Agencia Internacional de Energía Atómica. Este incidente resalta la compleja intersección entre la tecnología, seguridad y medio ambiente en medio de la controversia sobre Fukushima.

Prioridad: 3 Importante.

Ampliar información:

- https://www.genbeta.com/actualidad/grupo-hacker-ataca-21-sitios-web-gobierno-japon-protesta-liberacion-aguas-residuales-fukushima

---

Cuidado con Google Maps: cualquiera puede cambiar en su favor los datos de los mapas.

Google Maps permite a los usuarios sugerir cambios en la información, lo que puede ser explotado para vandalismo o estafas al alterar horarios y datos de contacto. Ya ha ocurrido en el pasado que los ciberdelincuentes cambiaron números de teléfono de sucursales bancarias para estafas.

Prioridad: 3 Importante.

Ampliar información:

- https://www.genbeta.com/seguridad/cuidado-google-maps-puede-cambiar-su-favor-datos-mapas-asi-ha-sufrido-esta-localidad-granada

---

VPNs podrían ser vulnerables a ataque TunnelCrack que amenaza la privacidad

Un equipo de investigadores ha revelado la existencia de una serie de técnicas llamadas TunnelCrack, que en ciertas condiciones pueden ser utilizadas para forzar el tráfico de red de las víctimas a salir de sus conexiones VPN encriptadas. Esto podría permitir a los atacantes observar el tráfico en la red local. Los investigadores probaron más de 60 clientes VPN y descubrieron que todas las aplicaciones VPN en iOS son vulnerables, mientras que Android parece ser más seguro. Los ataques, conocidos como LocalNet y ServerIP, explotan fallas en la configuración de los dispositivos y clientes VPN. Varios proveedores VPN han respondido a esta vulnerabilidad, algunos implementando soluciones y otras evaluando su impacto.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.theregister.com/2023/08/10/tunnelcrack_vpn/?&web_view=true

---

Google presenta la primera implementación de clave de seguridad FIDO2 resiliente cuántica

Google ha lanzado la primera llave de seguridad FIDO2 resistente a la computación cuántica como parte de su iniciativa OpenSK. Esta llave utiliza un esquema de firma híbrida que combina ECC y Dilithium para brindar seguridad contra ataques estándar y cuánticos. OpenSK es una implementación de código abierto escrita en Rust que respalda los estándares FIDO U2F y FIDO2. Google espera que esta solución se estandarice para proteger las credenciales de los usuarios contra ataques cuánticos.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/08/google-introduces-first-quantum.html?&web_view=true

---