GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4924

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
VULNERABILIDADES	3	1	0
MALWARE	1	1	1
NOTICIAS DE CIBERSEGURIDAD	1	0	3

VULNERABILIDADES

Se descubren vulnerabilidades críticas en un punto de acceso inalámbrico industrial

Investigadores de Nozomi Networks Labs han identificado 20 vulnerabilidades en el punto de acceso inalámbrico industrial Advantech EKI-6333AC-2G, seis de las cuales son críticas y permiten la ejecución remota de código con privilegios de root. Estas vulnerabilidades, presentes en entornos industriales como líneas de ensamblaje automotriz y operaciones logísticas, pueden comprometer la confidencialidad, integridad y disponibilidad de los dispositivos afectados. Cada vulnerabilidad ha recibido un identificador CVE único, incluyendo CVE-2024-50370, CVE-2024-50371, CVE-2024-50372, CVE-2024-50373, CVE-2024-50374 y CVE-2024-50375.

Advantech ha lanzado actualizaciones de firmware para mitigar estos riesgos, instando a los usuarios a actualizar a las versiones v1.6.5 para EKI-6333AC-2G y EKI-6333AC-2GD, y

v1.2.2 para EKI-6333AC-1GPO. La explotación de estas vulnerabilidades podría realizarse a través de la red o mediante proximidad física, permitiendo a atacantes ejecutar código malicioso para realizar actividades como acceso persistente, robo de datos y alteración de operaciones en la red.

Prioridad: Crítico

Ampliar información:

https://www.infosecurity-magazine.com/news/critical-vulnerabilities/

Falta autenticación en fgfmsd

Fortinet ha identificado una vulnerabilidad crítica en su plataforma FortiManager, específicamente en el fgfmsd daemon, que gestiona la comunicación entre FortiManager y dispositivos FortiGate. Esta falla, catalogada como CVE-2024-47575, permite a atacantes remotos no autenticados ejecutar código o comandos arbitrarios mediante solicitudes especialmente diseñadas.

La explotación de esta vulnerabilidad ha sido observada en entornos reales, donde actores malintencionados han utilizado dispositivos FortiManager no autorizados para extraer datos de configuración y contraseñas cifradas de dispositivos FortiGate gestionados. Fortinet ha lanzado actualizaciones de firmware para mitigar este riesgo y recomienda a los usuarios actualizar a las versiones corregidas correspondientes.

Prioridad: Crítico

Ampliar información:

https://www.fortiguard.com/psirt/FG-IR-24-423

Detectadas varias vulnerabilidades importantes en productos QNAP

El Instituto Nacional de Ciberseguridad (INCIBE) ha reportado múltiples vulnerabilidades críticas sobre productos QNAP, incluidos Notes Station 3, QNAP AI Core, QTS, QuTS hero y QuLog Center, con identificadores CVE asignados como CVE-2024-38643, CVE-2024-38647, CVE-2024-37044, CVE-2024-37045, CVE-2024-37046, CVE-2024-48860, y CVE-2024-48862. Estas fallas abarcan problemas como ejecución de código remoto, exposición de información sensible, inyección de comandos, y gestión incorrecta de permisos. Los riesgos incluyen el compromiso total del sistema, acceso no autorizado a datos confidenciales, y ataques de denegación de servicio.

QNAP ha lanzado actualizaciones de firmware para abordar estas vulnerabilidades e insta a los usuarios a aplicar las últimas versiones de software. Asimismo, recomienda restringir el acceso a dispositivos afectados hasta implementar los parches. La actualización inmediata y el seguimiento de las mejores prácticas de ciberseguridad son esenciales para mitigar los riesgos asociados a estas vulnerabilidades.

Prioridad: Crítico

Ampliar información:

https://www.incibe.es/empresas/avisos/detectadas-varias-vulnerabilidades-importantes-en-productos-qnap

---

Microsoft corrige vulnerabilidad explotada en sitio web de red de socios

Microsoft ha corregido recientemente una vulnerabilidad crítica en su sitio web de la Red de Socios, específicamente en el dominio 'partner.microsoft.com'. Identificada como CVE-2024-49035, esta vulnerabilidad de control de acceso inadecuado permitía a atacantes no autenticados escalar privilegios a través de la red. Microsoft ha confirmado que esta falla fue explotada, aunque no ha proporcionado detalles adicionales sobre los ataques.

Además de esta corrección, la compañía ha abordado otras vulnerabilidades en servicios como Azure y Copilot Studio. Sin embargo, los clientes no necesitan realizar acciones

específicas, ya que las actualizaciones se implementan automáticamente y ha asignado identificadores CVE a estas vulnerabilidades.

Prioridad: Urgente

Ampliar información:

https://www.securityweek.com/microsoft-patches-exploited-vulnerability-in-partner-network-website/

Recomendaciones generales sobre vulnerabilidades:

Para reducir las vulnerabilidades en los sistemas, se sugieren las siguientes acciones clave:

Aplicar parches de seguridad de forma regular para solucionar fallos conocidos.

Añadir una capa adicional de seguridad, como la autenticación de dos factores (2FA), para complicar el acceso no autorizado.

Restringir los permisos de usuarios y aplicaciones, limitando el acceso solo a lo necesario para reducir riesgos.

Utilizar herramientas de detección de intrusiones para monitorizar y detectar comportamientos sospechosos.

Estas medidas son esenciales para contribuir a fortalecer la seguridad de los sistemas.

MALWARE

Se descubre que la biblioteca Python de PyPI "aiocpa" filtra claves criptográficas mediante un bot de Telegram

Investigadores de ciberseguridad han descubierto que la biblioteca de Python "aiocpa", disponible en el repositorio PyPI, contenía código malicioso diseñado para exfiltrar claves privadas de criptomonedas a través de un bot de Telegram. Este paquete, presentado como un cliente para la API de Crypto Pay, fue lanzado en septiembre de 2024 y acumuló más de 12,000 descargas antes de que se detectara la amenaza.

La versión 0.1.13 de "aiocpa" introdujo un script ofuscado que, al ejecutarse, enviaba información sensible, como tokens y datos relacionados con Crypto Pay, a un bot de Telegram controlado por los atacantes. Curiosamente, el repositorio de GitHub asociado al proyecto no mostraba signos de esta actividad maliciosa, lo que sugiere un intento deliberado de evadir la detección. Tras ser alertado, PyPI puso en cuarentena el paquete para prevenir futuras instalaciones y modificaciones por parte de sus mantenedores.

Prioridad: Crítico

Ampliar información:

https://thehackernews.com/2024/11/pypi-python-library-aiocpa-found.html

---

Hackers de Salt Typhoon introducen el nuevo malware GhostSpider en las empresas de telecomunicaciones

El grupo de ciberespionaje patrocinado por el estado chino, conocido como Salt Typhoon (también denominado 'Earth Estries', 'GhostEmperor' o 'UNC2286'), ha desplegado un nuevo backdoor llamado GhostSpider en ataques dirigidos a proveedores de servicios de telecomunicaciones. Este backdoor, descubierto por Trend Micro, permite a los atacantes mantener un acceso persistente a los sistemas comprometidos, facilitando la exfiltración de datos sensibles y la manipulación del sistema operativo.

Además de GhostSpider, Salt Typhoon emplea otras herramientas maliciosas como el backdoor para Linux 'Masol RAT', el rootkit 'Demodex' y el backdoor modular 'SnappyBee', compartido entre grupos APT chinos. Estas herramientas refuerzan las capacidades del

grupo para llevar a cabo operaciones de espionaje a largo plazo, destacando la sofisticación y persistencia de sus campañas contra infraestructuras críticas y entidades gubernamentales a nivel mundial.

Prioridad: Urgente

Ampliar información:

https://www.bleepingcomputer.com/news/security/salt-typhoon-hackers-backdoor-telcos-with-new-ghostspider-malware/

Investigadores descubren «Bootkitty», el primer bootkit UEFI dirigido a núcleos Linux

Investigadores de ESET han descubierto Bootkitty, el primer bootkit UEFI diseñado específicamente para sistemas Linux, marcando una evolución significativa en el panorama de amenazas, ya que anteriormente estos bootkits se dirigían principalmente a sistemas Windows. Este malware compromete el proceso de arranque del sistema, permitiendo a los atacantes desactivar la verificación de firmas del kernel y cargar binarios maliciosos durante el inicio, lo que facilita la evasión de medidas de seguridad tradicionales.

Aunque actualmente se considera una prueba de concepto y no se ha detectado en ataques reales, Bootkitty destaca la creciente sofisticación de las amenazas dirigidas a plataformas Linux. Su capacidad para modificar funciones críticas del proceso de arranque y cargar módulos del kernel no firmados subraya la necesidad de fortalecer las defensas en sistemas Linux, incluyendo la habilitación de Secure Boot y la implementación de medidas de seguridad adicionales para proteger contra este tipo de amenazas avanzadas.

Prioridad: Importante

Ampliar información:

https://thehackernews.com/2024/11/researchers-discover-bootkitty-first.html

---

Recomendaciones generales sobre malware:

Para protegerse del malware, es fundamental:

Mantener el software y los sistemas operativos actualizados de manera regular, ya que los atacantes suelen aprovechar vulnerabilidades en versiones obsoletas.

Utilizar programas antivirus y antimalware confiables, asegurándose de que siempre estén actualizados.

Activar la autenticación multifactor (MFA) para asegurar cuentas sensibles y dificultar el acceso no autorizado.

Ser cauteloso con correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de infección por malware.

Hacer copias de seguridad periódicas de los archivos importantes, para evitar pérdidas en caso de ataques como el ransomware.

Restringir los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

El nuevo servicio de phishing 2FA de Rockstar ataca las cuentas de Microsoft 365

Un nuevo servicio de phishing como servicio (PhaaS) denominado 'Rockstar 2FA' ha surgido, facilitando ataques de adversario en el medio (AiTM) a gran escala para robar credenciales de Microsoft 365. Este servicio permite a los atacantes eludir las protecciones de autenticación multifactor (MFA) al interceptar cookies de sesión válidas. El ataque funciona redirigiendo a las víctimas a una página de inicio de sesión falsa que imita a

Microsoft 365, engañándolas para que ingresen sus credenciales. El servidor AiTM actúa como un proxy, transmitiendo esas credenciales al servicio legítimo de Microsoft para completar el proceso de autenticación y luego captura la cookie cuando se envía de vuelta al navegador de la víctima. Esta cookie puede ser utilizada por los actores de amenazas para acceder directamente a la cuenta de la víctima, incluso si está protegida por MFA, sin necesidad de las credenciales.

Según Trustwave, 'Rockstar 2FA' es una evolución de kits de phishing previos como DadSec y Phoenix, ganando popularidad entre actores maliciosos desde agosto de 2024. Este servicio se vende por $200 USD para dos semanas de uso y ofrece renovaciones por $180 USD, consolidándose como una herramienta accesible y peligrosa.

Prioridad: Crítico

Ampliar información:

https://www.bleepingcomputer.com/news/security/new-rockstar-2fa-phishing-service-targets-microsoft-365-accounts/

Las empresas de criptomonedas están siendo afectadas por ataques deepfake

Un estudio reciente de Regula revela que el sector de las criptomonedas enfrenta un aumento significativo en fraudes mediante deepfakes, superando incluso al fraude tradicional con documentos falsificados. El 57% de las empresas de criptomonedas reportan incidentes relacionados con deepfakes de audio, mientras que el 53% han enfrentado fraudes con deepfakes de video. Estas cifras contrastan con otros sectores, donde el fraude con documentos falsos sigue siendo la principal amenaza.

Las pérdidas promedio en la industria de criptomonedas debido a estas técnicas avanzadas de fraude ascienden a $440,000 USD, y un 37% de las empresas afectadas reportan pérdidas superiores a $500,000 USD. Para contrarrestar estas amenazas, el 90% de las empresas de criptomonedas priorizan entrevistas en video en vivo combinadas con

verificación de documentos como estrategia principal de prevención de fraude. Además, el 39% aboga por la creación de un organismo regulador dedicado a monitorear y combatir las amenazas relacionadas con deepfakes, superando el promedio global del 29%.

Prioridad: Importante

Ampliar información:

https://www.helpnetsecurity.com/2024/11/28/crypto-deepfake-fraud/

Informe de tendencias de APT del tercer trimestre de 2024

El informe de Kaspersky del tercer trimestre de 2024 destaca actividades significativas de grupos APT, incluyendo operaciones de hacktivismo, desarrollo de nuevas herramientas y campañas dirigidas. Se observó un aumento en la actividad de grupos como SideWinder, que ha ampliado sus objetivos en el Medio Oriente y África, y BlindEagle, que continúa atacando a organizaciones en América Latina. Además, se identificaron campañas como EastWind, que emplea herramientas como CloudSorcerer para atacar a organizaciones gubernamentales en Rusia.

El informe también resalta la evolución de las técnicas utilizadas por estos grupos, incluyendo el uso de servicios en la nube para el comando y control, y la implementación de nuevos backdoors y troyanos de acceso remoto.

Prioridad: Importante

Ampliar información:

https://securelist.com/apt-report-q3-2024/114623/

Ciberataque expone datos de usuarios personales del RAIA

El Consejo Andaluz de Colegios Oficiales de Veterinarios ha informado sobre un ciberataque al Registro Andaluz de Identificación Animal (RAIA), comprometiendo datos personales de propietarios de mascotas, como nombre, apellidos, documentos de identificación, dirección, teléfono y correo electrónico. Aunque no se afectaron datos financieros ni contraseñas, la exposición de esta información podría facilitar fraudes o ataques de ingeniería social.

Tras detectar el incidente, se notificó a la Agencia Española de Protección de Datos y se enviaron alertas vía SMS a los afectados, aconsejando precaución ante comunicaciones sospechosas y evitando interactuar con enlaces dudosos en correos electrónicos, SMS o WhatsApp. El Consejo ha reforzado sus medidas de ciberseguridad y ofrece asistencia a través de su delegado de protección de datos.

Prioridad: Importante

Ampliar información:

https://unaaldia.hispasec.com/2024/11/ciberataque-expone-datos-de-usuarios-personales-del-registro-andaluz-de-identificacion-animal-raia.html