GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1125

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
VULNERABIILIDADES	0	1	2
MALWARE	0	2	1
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Ciberdelincuentes usan CSS para evadir filtros de spam y rastrear usuarios de email

Investigadores de Cisco Talos han descubierto que ciberdelincuentes están explotando características de las Hojas de Estilo en Cascada (CSS) para evadir filtros de spam y rastrear las acciones de los usuarios en correos electrónicos. Estas tácticas permiten a los atacantes comprometer la seguridad y privacidad de las víctimas al utilizar propiedades de CSS como text-indent y opacity para ocultar contenido irrelevante en el cuerpo del correo electrónico, con el objetivo de redirigir a los destinatarios a páginas de phishing.

Además, los atacantes emplean reglas CSS como @media para monitorear el comportamiento de los usuarios, incluyendo preferencias de fuente, esquema de colores y acciones como la visualización o impresión de correos electrónicos. Para mitigar estos riesgos, se recomienda implementar mecanismos avanzados de filtrado que detecten

técnicas de ocultamiento de contenido y utilizar proxies de privacidad en el correo electrónico.

Prioridad: Urgente.

Ampliar Información:

https://thehackernews.com/2025/03/cybercriminals-exploit-css-to-evade.html

---

Falla en Cisco IOS XR permite ataques de denegación de servicio en BGP

Cisco ha solucionado una vulnerabilidad de denegación de servicio (DoS) identificada como CVE-2025-20115, que afecta a los routers que ejecutan IOS XR con la funcionalidad de confederación BGP habilitada. Esta vulnerabilidad permite a atacantes no autenticados causar una corrupción de memoria mediante un desbordamiento de búfer, lo que provoca el reinicio del proceso BGP en dispositivos vulnerables.

La explotación exitosa de esta falla puede lograrse enviando un mensaje BGP especialmente diseñado con un atributo AS_CONFED_SEQUENCE que contenga 255 números de sistema autónomo (AS). Este ataque de baja complejidad puede ser ejecutado de forma remota, lo que representa un riesgo significativo para la estabilidad de las redes afectadas. Se recomienda a quienes utilizan dispositivos Cisco IOS XR con confederaciones BGP que apliquen las actualizaciones de seguridad proporcionadas por Cisco para mitigar esta vulnerabilidad.

Prioridad: Importante.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/cisco-vulnerability-lets-attackers-crash-bgp-on-ios-xr-routers/

Una falla sin parchear en la cámara Edimax se ha explotado para ataques de botnet Mirai

Una vulnerabilidad crítica identificada como CVE-2025-1316 afecta a las cámaras IP Edimax IC-7100, permitiendo a atacantes remotos ejecutar código arbitrario mediante solicitudes especialmente diseñadas. Desde mayo de 2024, esta vulnerabilidad ha sido explotada por variantes del malware Mirai para comprometer dispositivos y formar redes botnet utilizadas en ataques de denegación de servicio distribuido (DDoS).

Dado que estos dispositivos fueron descontinuados hace más de una década y no recibirán actualizaciones de seguridad, se recomienda a los usuarios afectados reemplazarlos por modelos más recientes. Mientras tanto, es aconsejable evitar exponer estas cámaras directamente a internet, cambiar las contraseñas predeterminadas y monitorear los registros de acceso en busca de actividades inusuales.

Prioridad: Importante.

Ampliar Información:

https://thehackernews.com/2025/03/unpatched-edimax-camera-flaw-exploited.html

---

Recomendaciones Generales Sobre Vulnerabilidades:

Para mitigar las vulnerabilidades en los sistemas, se recomiendan las siguientes medidas claves.

1. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.
2. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.
3. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.

4. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.
5. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

Paquetes maliciosos en PyPI roban tokens en la nube y acumulan más de 14,100 descargas antes de ser eliminados

Investigadores han identificado una campaña maliciosa dirigida a usuarios del Python Package Index (PyPI), en la cual se distribuyeron bibliotecas falsas que aparentaban ser utilidades relacionadas con el tiempo, pero que en realidad contenían funcionalidades ocultas para robar datos sensibles, como tokens de acceso a servicios en la nube.

La empresa de seguridad de la cadena de suministro de software ReversingLabs descubrió dos conjuntos de paquetes maliciosos que, en conjunto, sumaban 20 paquetes y acumularon más de 14,100 descargas antes de ser eliminados de PyPI. El primer conjunto incluía paquetes como snapshot-photo y time-check-server, diseñados para cargar datos en la infraestructura del atacante. El segundo conjunto consistía en paquetes que implementaban funcionalidades de clientes en la nube para servicios como Alibaba Cloud, Amazon Web Services y Tencent Cloud, pero que también exfiltraban secretos de la nube. Algunos de estos paquetes maliciosos fueron listados como dependencias en proyectos populares de GitHub, lo que facilitó su propagación.

Este incidente resalta la importancia de que los desarrolladores verifiquen la autenticidad y seguridad de las dependencias que integran en sus proyectos, especialmente cuando provienen de repositorios públicos. Además, se recomienda monitorear regularmente las dependencias utilizadas y aplicar medidas de seguridad para mitigar riesgos asociados a la cadena de suministro de software.

Prioridad: Urgente.

https://thehackernews.com/2025/03/malicious-pypi-packages-stole-cloud.html

---

Grupo de ransomware desarrolla herramienta para automatizar ataques de fuerza bruta

El grupo de ransomware Black Basta ha desarrollado una herramienta automatizada llamada BRUTED para realizar ataques de fuerza bruta contra dispositivos de red perimetrales, como firewalls y VPNs. Esta herramienta permite al grupo escalar sus ataques de ransomware al obtener acceso inicial a redes a través de dispositivos expuestos a internet.

El análisis del código fuente de BRUTED revela que está diseñada específicamente para atacar productos de VPN y acceso remoto, incluyendo SonicWall NetExtender, Palo Alto GlobalProtect, Cisco AnyConnect, Fortinet SSL VPN, Citrix NetScaler (Citrix Gateway), Microsoft RDWeb (Remote Desktop Web Access) y WatchGuard SSL VPN.

Se recomienda reforzar las medidas de seguridad, implementar autenticación multifactor y asegurarse que las configuraciones de los dispositivos de red estén actualizadas para mitigar posibles ataques.

Prioridad: Urgente.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/black-basta-ransomware-creates-automated-tool-to-brute-force-vpns/

MassJacker: nuevo malware que ataca a piratas y roba criptomonedas

El malware MassJacker es una amenaza reciente que se dirige a usuarios que buscan software pirata, con el objetivo de robar criptomonedas mediante la manipulación del

contenido del portapapeles. Este tipo de malware, conocido como "clipper", monitorea el portapapeles de la víctima y reemplaza las direcciones de billeteras de criptomonedas copiadas por otras controladas por los atacantes, redirigiendo así las transacciones a sus propias cuentas.

La cadena de infección comienza en el sitio web pesktop[.]com, que se presenta como una fuente de software pirata, pero en realidad distribuye malware. Al descargar e instalar el software desde este sitio, se ejecuta un script de PowerShell que instala el malware Amadey, junto con otros binarios que finalmente inyectan el payload de MassJacker en un proceso legítimo de Windows, como "InstalUtil.exe".

MassJacker implementa técnicas avanzadas de evasión y anti-análisis, incluyendo Just-In-Time (JIT) hooking, mapeo de tokens de metadatos para ocultar llamadas a funciones y una máquina virtual personalizada para interpretar comandos en lugar de ejecutar código .NET regular. Además, realiza comprobaciones anti-depuración y se configura para identificar patrones de expresiones regulares que coincidan con direcciones de billeteras de criptomonedas en el portapapeles. Una vez detecta una dirección, la reemplaza por una perteneciente a los atacantes, descargada previamente desde un servidor remoto.

Prioridad: Importante.

Ampliar Información:

https://thehackernews.com/2025/03/new-massjacker-malware-targets-piracy.html

---

Recomendaciones Generales Sobre Malware:

Para protegerse contra malware, es esencial

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.

2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.
7.

NOTICIAS DE CIBERSEGURIDAD

Millones de tarjetas bancarias filtradas en la Dark Web

Según un informe de Kaspersky, se han detectado 2,3 millones de tarjetas bancarias filtradas en la Dark Web entre 2023 y 2024. Esta filtración masiva expone a millones de usuarios al riesgo de fraudes financieros y destaca la creciente amenaza que representan las brechas de seguridad en el sector bancario

La exposición de datos sensibles en mercados clandestinos subraya la necesidad urgente de reforzar las medidas de ciberseguridad en las instituciones financieras. Es esencial implementar estrategias proactivas para proteger la información confidencial de los clientes y mitigar el impacto de posibles ataques cibernéticos.

Prioridad: Importante

Ampliar Información:

https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/informe-kaspersky-23-millones-de-tarjetas-bancarias-filtradas-en-la-dark

La Agencia Espacial Polaca fuera de servicio tras un ciberataque

La Agencia Espacial Polaca (POLSA) sufrió un ciberataque que comprometió su infraestructura de TI, lo que llevó a la desconexión inmediata de su red de Internet para proteger los datos y contener el incidente. Las autoridades polacas están llevando a cabo una investigación exhaustiva para identificar a los responsables, en medio de crecientes tensiones geopolíticas y acusaciones previas hacia Rusia por intentos de desestabilización debido al apoyo de Polonia a Ucrania.

Este ataque subraya la vulnerabilidad de las instituciones estratégicas a las amenazas cibernéticas y la necesidad de fortalecer las medidas de seguridad en sectores críticos. La desconexión preventiva de POLSA destaca la importancia de contar con protocolos de respuesta efectivos para minimizar el impacto de tales incidentes en la seguridad nacional y la continuidad operativa.

Prioridad: Importante.

Ampliar Información:

https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/la-agencia-espacial-polaca-fuera-de-servicio-tras-un-ciberataque