GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °1724

En alianza con

TD SYNNEX FORTINET

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	2	2	2
MALWARE	0	1	5
NOTICIAS DE CIBERSEGURIDAD	0	0	3

VULNERABILIDADES

Vulnerabilidad de ejecución de código remoto no autenticado en LobalProtect está siendo explotada el mismo día en que se descubrió

El 10 de abril de 2024, Volexity identificó la explotación de una vulnerabilidad de día cero en la función GlobalProtect de Palo Alto Networks PAN-OS en uno de sus clientes de monitoreo de seguridad de red (NSM). Volexity recibió alertas sobre tráfico de red sospechoso proveniente del firewall del cliente. Una investigación posterior reveló que el dispositivo había sido comprometido. Al día siguiente, el 11 de abril de 2024, Volexity observó explotaciones adicionales y similares en otro cliente de NSM por parte del mismo actor de amenazas.

Prioridad: 1 Crítico.

Ampliar información:

https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400

Palo Alto Networks soluciona vulnerabilidad de día cero explotada para instalar puertas traseras en firewalls

Palo Alto Networks ha iniciado la distribución de parches de emergencia para una vulnerabilidad de día cero que ha sido activamente aprovechada desde el 26 de marzo para implantar puertas traseras en los firewalls PAN-OS. Esta vulnerabilidad crítica (CVE-2024-3400) afecta a los firewalls PAN-OS 10.2, PAN-OS 11.0 y PAN-OS 11.1 con la telemetría del dispositivo y GlobalProtect (gateway o portal) habilitados.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/04/palo-alto-networks-releases-urgent.html

---

Ivanti advierte sobre fallos críticos en su solución de MDM Avalanche

Ivanti ha emitido actualizaciones de seguridad para corregir 27 vulnerabilidades en su solución de gestión de dispositivos móviles (MDM) Avalanche, incluyendo dos desbordamientos críticos de montón que pueden ser aprovechados para ejecutar comandos de forma remota. Avalanche es utilizado por administradores empresariales para gestionar de manera remota, implementar software y programar actualizaciones en flotas extensas de más de 100,000 dispositivos móviles desde una única ubicación central.

Prioridad: 1 Crítico.

Ampliar información:

https://forums.ivanti.com/s/article/Avalanche-6-4-3-Security-Hardening-and-CVEs-addressed?language=en_US

Exploit para la vulnerabilidad de Palo Alto PAN-OS utilizada en ataques

Se ha hecho público el código de explotación para una vulnerabilidad de gravedad máxima que está siendo activamente aprovechada en el software de firewall PAN-OS de Palo Alto Networks. Identificada como CVE-2024-3400, esta falla de seguridad podría permitir que actores de amenazas no autenticados ejecuten código arbitrario como root mediante la inyección de comandos en ataques de baja complejidad dirigidos a firewalls vulnerables PAN-OS 10.2, PAN-OS 11.0 y PAN-OS 11.1, siempre que la telemetría del dispositivo y la función Global Protect (gateway o portal) estén habilitadas.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/exploit-released-for-palo-alto-pan-os-bug-used-in-attacks-patch-now/

La falla en el cliente SSH PuTTY permite la recuperación de claves privadas criptográficas

Una vulnerabilidad, identificada como CVE-2024-31497, en PuTTY 0.68 hasta 0.80 podría permitir que atacantes con acceso a 60 firmas criptográficas recuperen la clave privada utilizada para su generación. PuTTY es un popular emulador de terminal de código abierto, consola serial y aplicación de transferencia de archivos de red que admite SSH (Secure Shell), Telnet, SCP (Secure Copy Protocol) y SFTP (SSH File Transfer Protocol).

Prioridad: 3 Importante.

Ampliar información:

https://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-p521-bias.html

---

Las botnets continúan explotando CVE-2023-1389 para una propagación a gran escala

El año pasado se dio a conocer una vulnerabilidad de inyección de comandos, identificada como CVE-2023-1389, y se desarrolló una solución para la interfaz de gestión web del TP-Link Archer AX21 (AX1800). FortiGuard Labs ha creado una firma de IPS para abordar este problema. Recientemente, hemos observado múltiples ataques dirigidos a esta vulnerabilidad de hace un año, destacando botnets como Moobot, Miroi, el agente basado en Golang "AGoent" y la Variante Gafgyt.

Prioridad: 3 Importante.

Ampliar información:

https://www.fortinet.com/blog/threat-research/botnets-continue-exploiting-cve-2023-1389-for-wide-scale-spread

---

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

Contenedor Rust Backdoor XZ

Se ha difundido ampliamente la noticia sobre la puerta trasera maliciosa encontrada en la biblioteca de compresión XZ Utils. Aunque el posible daño parece haber sido en gran medida mitigado por el trabajo de un solo ingeniero, aún persisten réplicas de este ataque. El tema de hoy trata sobre una de esas réplicas encontradas en el ecosistema de Rust por Phylum, así como la rápida acción tomada por el mantenedor del contenedor Rust, y los peligros que podrían persistir.

Prioridad: 2 Urgente.

Ampliar información:

https://blog.phylum.io/rust-crate-shipping-xz-backdoor

Uso de LockBit Builder para generar ransomware dirigido

La investigación previa de Kaspersky se enfocó en un análisis detallado del constructor filtrado de LockBit 3.0 en 2022. Desde entonces, los atacantes han sido capaces de generar versiones personalizadas de la amenaza de acuerdo con sus necesidades. Esto abre numerosas posibilidades para que los actores maliciosos hagan que sus ataques sean más efectivos, ya que pueden configurar opciones de propagación en la red y funcionalidades para desactivar las defensas. Esto se vuelve aún más peligroso si el atacante cuenta con credenciales privilegiadas válidas en la infraestructura objetivo.

Prioridad: 3 Importante.

Ampliar información:

https://securelist.com/lockbit-3-0-based-custom-targeted-ransomware/112375

Actividad de fuerza bruta a gran escala dirigida a VPN y servicios SSH con credenciales de inicio

Cisco Talos está actualmente monitoreando un aumento global en los ataques de fuerza bruta dirigidos a una variedad de objetivos, incluyendo servicios de Red Privada Virtual (VPN), interfaces de autenticación de aplicaciones web y servicios SSH desde al menos el 18 de marzo de 2024. Estos ataques parecen estar siendo originados desde nodos de salida de TOR, una variedad de otros túneles y proxies de anonimización.

Prioridad: 3 importante.

Ampliar información:

https://blog.talosintelligence.com/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials/

Ransomware Cerber

Cado Security Labs recientemente recibió informes sobre el ransomware Cerber siendo desplegado en servidores que ejecutan la aplicación Confluence mediante la explotación de CVE-2023-22518. Aunque existe una amplia cobertura sobre la variante de Windows, hay escasa información disponible sobre la variante de Linux. En este blog, discutiremos un análisis de la variante de Linux.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/04/critical-atlassian-flaw-exploited-to.html

---

El grupo de amenazas FIN7 apunta a la industria automotriz de EE. UU.

A fines de 2023, los analistas de BlackBerry identificaron una campaña de spear-phishing llevada a cabo por el grupo de amenazas FIN7, dirigida a un importante fabricante de automóviles con sede en Estados Unidos. FIN7 identificó a empleados de la empresa que trabajaban en el departamento de TI y tenían niveles más altos de derechos administrativos. Utilizaron el reclamo de una herramienta gratuita de escaneo de IP para ejecutar su conocida puerta trasera Anunak y obtener un punto de apoyo inicial mediante el uso de binarios, scripts y bibliotecas de "living off the land" (lolbas). También hemos encontrado evidencia de que este ataque formaba parte de una campaña más amplia llevada a cabo por FIN7.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/fin7-targets-american-automakers-it-staff-in-phishing-attacks/

Comentarios sobre GitHub utilizados para distribuir malware a través de URL de repositorios de Microsoft

Una vulnerabilidad en GitHub, o posiblemente una decisión de diseño, está siendo explotada por actores de amenazas para distribuir malware utilizando URLs asociadas a un repositorio de Microsoft, lo que hace que los archivos parezcan confiables. Aunque la mayoría de la actividad de malware se ha centrado en las URLs de GitHub de Microsoft, esta "vulnerabilidad" podría ser aprovechada con cualquier repositorio público en GitHub, lo que permite a los actores de amenazas crear señuelos muy convincentes.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/github-comments-abused-to-push-malware-via-microsoft-repo-urls/

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

Orientación conjunta sobre la implementación segura de sistemas de inteligencia artificial

El Centro de Seguridad de la Inteligencia Artificial (AISC) de la Agencia de Seguridad Nacional (NSA) publicó la Hoja de Información Conjunta de Ciberseguridad sobre la Implementación Segura de Sistemas de IA en colaboración con CISA, el Buró Federal de Investigación (FBI), el Centro de Seguridad Cibernética Australiano (ASD ACSC) de la Dirección de Señales de Australia, el Centro Canadiense de Ciberseguridad (CCCS), el Centro Nacional de Ciberseguridad de Nueva Zelanda (NCSC-NZ) y el Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC-UK).

Prioridad: 3 Importante.

Ampliar información:

https://www.cisa.gov/news-events/alerts/2024/04/15/joint-guidance-deploying-ai-systems-securely

---

El FBI informa que hackers chinos se están preparando para atacar la infraestructura de EE. UU.

El jueves, el director del FBI, Christopher Wray, advirtió que hackers vinculados al gobierno chino se han infiltrado en la infraestructura crítica de Estados Unidos y están esperando el momento oportuno para lanzar un ataque devastador. Según Wray, una campaña continua de piratería china, conocida como Volt Typhoon, ha logrado acceder con éxito a numerosas empresas estadounidenses en sectores clave como telecomunicaciones, energía, agua, entre otros, poniendo también como objetivo a 23 operadores de oleoductos. Estas declaraciones las realizó durante un discurso en la Universidad Vanderbilt.

Prioridad: 3 Importante.

Ampliar información:

https://www.itnews.com.au/news/fbi-says-chinese-hackers-preparing-to-attack-us-infrastructure-607271

Cómo los atacantes pueden controlar un negocio sin necesidad de tocar el punto final

Los ciberatacantes están empleando cada vez más técnicas de ataque "sin red" dirigidas a aplicaciones en la nube e identidades. Este artículo explica cómo los atacantes pueden comprometer organizaciones sin necesidad de acceder a los puntos finales ni a los sistemas y servicios de red convencionales.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/04/showcasing-networkless-identity-attacks.html

---