GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2624

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	1	1
MALWARE	0	1	3
NOTICIAS DE CIBERSEGURIDAD	0	0	4

VULNERABILIDADES

Vulnerabilidades críticas en vCenter Server CVE-2024-37079, CVE-2024-37080, CVE-2024-37081

VMware ha lanzado parches para tres vulnerabilidades críticas en vCenter Server. Estas vulnerabilidades incluyen la ejecución remota de código y la escalada de privilegios locales, afectando a empresas que utilizan vCenter Server para gestionar entornos vSphere.

Detalles de las Vulnerabilidades:

1. CVE-2024-37079: Vulnerabilidad de desbordamiento de heap en el protocolo DCERPC, permitiendo la ejecución remota de código. (CVSS v3.1: 9.8, crítica)
2. CVE-2024-37080: Similar a la anterior, otro desbordamiento de heap en DCERPC, permitiendo la ejecución remota de código. (CVSS v3.1: 9.8, crítica)
3. CVE-2024-37081: Configuración incorrecta de sudo que permite la elevación de privilegios a root por parte de un usuario local autenticado. (CVSS v3.1: 7.8, alta)

Prioridad: 1 Crítica.

Ampliar información:

https://unaaldia.hispasec.com/2024/06/vmware-parche-para-tres-vulnerabilidades-criticas.html

---

Vulnerabilidad de Microsoft Outlook CVE-2024-30103

Recientemente se ha identificado una vulnerabilidad en Microsoft Outlook CVE-2024-30103. Es una vulnerabilidad de ejecución remota de código (RCE) de "zero-click" que puede ser explotada simplemente al abrir o previsualizar un correo electrónico con una carga maliciosa, sin necesidad de interacción adicional del usuario.

Prioridad: 1 Crítica.

Ampliar información:

https://blog.segu-info.com.ar/2024/06/vulnerabilidad-critica-de-microsoft.html

---

Vulnerabilidad de Zero-Day en Chrome CVE-2024-6100

Google ha anunciado la actualización de Chrome 126, que incluye seis correcciones de seguridad, cuatro de las cuales abordan vulnerabilidades de alta severidad reportadas por investigadores externos. La vulnerabilidad más relevante, CVE-2024-6100, es un problema de confusión de tipos de alta severidad en el motor JavaScript V8. Estas actualizaciones tienen como objetivo mejorar la seguridad del navegador Chrome y mitigar los riesgos potenciales de explotación por parte de actores maliciosos.

Prioridad: 3 Importante.

Ampliar información:

https://www.securityweek.com/chrome-126-update-patches-vulnerability-exploited-at-hacking-competition/

Vulnerabilidad en Firmware de PC y Servidores UEFI CVE-2024-0762

Eclypsium Automata ha identificado una vulnerabilidad de alto impacto (CVE-2024-0762 con un CVSS reportado de 7.5) en el firmware Phoenix SecureCore UEFI que se encuentra en múltiples familias de procesadores Intel Core para escritorio y móviles. El problema radica en una variable insegura en la configuración del Trusted Platform Module (TPM), que podría provocar un desbordamiento de búfer y la ejecución potencial de código malicioso.

Prioridad: 2 Urgente.

Ampliar información:

https://eclypsium.com/blog/ueficanhazbufferoverflow-widespread-impact-from-vulnerability-in-popular-pc-and-server-firmware/

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

Nuevo Backdoor Oyester

Una campaña de malvertising está utilizando instaladores troyanizados de software popular como Google Chrome y Microsoft Teams para desplegar el backdoor Oyster. Según Rapid7, se han identificado sitios web falsos que alojan estas cargas maliciosas, a los que los usuarios son redirigidos tras buscar en Google y Bing. Oyster puede recolectar información del host, comunicarse con una dirección de comando y control (C2), y ejecutar código remotamente.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/06/oyster-backdoor-spreading-via.html

---

Malware RAT SneakyChef y SugarGhost

Talos Intelligence ha descubierto una sofisticada campaña cibernética atribuida al actor de amenazas SneakyChef, que utiliza el RAT SugarGh0st y otros programas maliciosos para atacar agencias gubernamentales, instituciones de investigación y organizaciones globales. La campaña, iniciada en agosto de 2023, comenzó con usuarios de Uzbekistán y Corea del Sur, pero se ha expandido a regiones como EMEA, Asia y Europa, incluyendo países como Angola, Turkmenistán, Kazajistán, India, Arabia Saudí, Letonia y Lituania. Los atacantes utilizan documentos señuelo, como circulares gubernamentales e invitaciones a conferencias de investigación, para atraer a sus víctimas.

Prioridad: 3 Importante.

Ampliar información:

https://gbhackers.com/new-rat-malware-sneakychef-sugarghost-attack-windows-systems/

Qilin Ransomware

Qilin (también conocido como Agenda) es una operación criminal de ransomware-as-a-service que colabora con afiliados para cifrar y exfiltrar datos de organizaciones hackeadas, exigiendo luego un rescate. A pesar de su nombre, derivado de una criatura mítica china, el grupo detrás de Qilin parece estar vinculado a Rusia. Activo desde octubre de 2022, Qilin ha atacado a organizaciones como The Big Issue, Yanfeng y el servicio judicial australiano. Recientemente, se declaró una "incidencia crítica" en varios hospitales de Londres tras un ataque de Qilin a la empresa de pruebas de sangre, Synnovis.

Prioridad: 3 Importante.

Ampliar información:

https://www.tripwire.com/state-of-security/qilin-ransomware-what-you-need-know

---

Operaciones de Espionaje de UNC3886

Después de descubrir malware en los hipervisores ESXi en septiembre de 2022, Mandiant comenzó a investigar múltiples intrusiones realizadas por UNC3886, un actor de ciberespionaje sospechoso de tener vínculos con China. Este grupo ha dirigido sus ataques hacia organizaciones estratégicas prominentes a nivel mundial. En enero de 2023, Mandiant proporcionó un análisis detallado sobre cómo el actor, utilizando una vulnerabilidad ya corregida en FortiOS, pudo llevar a cabo sus operaciones. Estos hallazgos resaltan las tácticas encubiertas y sofisticadas empleadas por UNC3886, subrayando la importancia de fortalecer la ciberseguridad en entornos corporativos y gubernamentales.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/06/chinese-cyber-espionage-group-exploits.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

La autenticación multifactor ya no es suficiente para proteger los datos en la nube

Durante el último mes, un grupo de ransomware, posiblemente vinculado a ShinyHunters o Scattered Spider, ha perpetrado varios ataques significativos. Primero, robaron más de 560 millones de registros de clientes de Ticketmaster, seguidos por 30 millones de cuentas del Banco Santander de España. Según Mandiant, las filtraciones no fueron resultado de vulnerabilidades, sino de credenciales comprometidas y controles deficientes en la autenticación multifactor (MFA), afectando a al menos otras 163 organizaciones.

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/cloud-security/multi-factor-authentication-not-enough-to-protect-cloud-data

Hacker revela método para infiltrarse en los sistemas de Santander y Ticketmaster

Después de las brechas de datos en el Banco Santander y Ticketmaster, donde millones de registros fueron filtrados y vendidos en la Dark Web, Wired ha logrado contactar a un ciberatacante del grupo ShinyHunters. Este hacker reveló que accedieron a los sistemas utilizando un servicio en la nube con acceso a las redes de ambos organismos. Este incidente subraya la creciente amenaza de ataques cibernéticos que comprometen la privacidad y seguridad de los usuarios en línea.

Prioridad: 3 Importante.

Ampliar información:

https://www.genbeta.com/actualidad/hacker-explica-como-irrumpieron-sistemas-santander-ticketmaster-pc-infectado-ucrania-fue-clave

---

UnitedHealth concluye revisión: "No hay evidencia de robo de registros médicos en ataque de ransomware"

UnitedHealth Group ha completado más del 90% de su revisión de los datos accedidos por los piratas informáticos de ransomware a principios de este año, no encontrando "ninguna evidencia" de exfiltración de historias clínicas o historiales médicos completos. El aviso de violación de datos, emitido el jueves, es la primera comunicación oficial a los afectados del ataque a Change Healthcare, que afectó severamente la industria médica. En abril, Change Healthcare confirmó el acceso de los piratas informáticos a datos personales de una gran cantidad de personas en EE.UU., incluyendo nombres, direcciones, fechas de nacimiento, números de teléfono y correos electrónicos, mientras continúan evaluando el alcance total del incidente.

Prioridad: 3 Importante.

Ampliar información:

https://thecyberpost.com/news/with-review-nearly-finished-unitedhealth-says-no-evidence-doctors-charts-stolen-in-ransomware-attack/

De experto tecnológico a líder en ciberseguridad: el camino hacia el liderazgo

Para un experto en tecnología, asumir un rol de liderazgo en ciberseguridad puede ser una oportunidad para influir y mejorar significativamente la postura de seguridad de su organización mediante cambios estratégicos e innovación. Además, puede acelerar el crecimiento profesional al desarrollar habilidades críticas y avanzar en un campo altamente valorado. Sin embargo, el miedo a la responsabilidad adicional, el temor al fracaso o la falta de confianza en las propias habilidades y calificaciones pueden ser barreras para dar el paso hacia este nuevo rol.

Prioridad: 3 Importante.

Ampliar información:

https://www.bankinfosecurity.com/blogs/making-move-from-tech-expert-to-cybersecurity-leader-p-3646