GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °2023

En alianza con

TD SYNNEX FORTINET

BOLETIN DE CIBERINTELIGENCIA DE AMENAZAS

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	7		
MALWARE			3
BRECHAS DE SEGURIDAD	1		
NOTICIAS DE CIBERSEGURIDAD		1	2
SECTOR GOBIERNO	1		

VULNERABILIDADES

Vulnerabilidad crítica en Foxit PDF Reader y Foxit PDF Editor (v12.1.2)

Tras el anuncio inicial de una vulnerabilidad crítica (CVE-2023-27363 con CVSSv3.2 9,8) que permitía la ejecución remota de código en Foxit Reader, recientemente se ha publicado una prueba de concepto funcional que permite llevar a cabo la explotación de dicha vulnerabilidad a través de la creación de un documento PDF especialmente manipulado.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.tarlogic.com/es/blog/cve-2023-27363-foxit-reader/
- https://www.foxit.com/support/security-bulletins.html
- https://github.com/j00sean/SecBugs/tree/main/CVEs/CVE-2023-27363 PoC (Prueba de Concepto)

Teléfonos Android son vulnerables a los ataques de fuerza bruta contra las huellas dactilares

BrutePrint es el nombre con el que los investigadores de la Universidad de Zhejiang y de Tencent Labs han bautizado al sistema con el cual pueden acceder a los móviles Android saltándose la protección con huella. A través de un ingenioso método, tienen la capacidad de desmantelar la hasta ahora férrea seguridad en la que confían millones de personas.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.adslzone.net/noticias/seguridad/barato-saltarse-proteccion-huella-movil-android/
- https://www.bleepingcomputer.com/news/security/android-phones-are-vulnerable-to-fingerprint-brute-force-attacks/

La vulnerabilidad en los cortafuegos Zyxel pronto puede ser ampliamente explotada (CVE-2023-28771)

Una vulnerabilidad de inyección de comandos recientemente reparada (CVE-2023-28771) que afecta a una variedad de firewalls Zyxel pronto podría ser explotada en la naturaleza, advirtieron los investigadores de Rapid7, después de publicar un análisis técnico y un script PoC que activa la vulnerabilidad y logra un shell de raíz inverso. .

Prioridad: 1 Crítico.

Ampliar información:

- https://www.helpnetsecurity.com/2023/05/22/cve-2023-28771/

Apple corrige tres nuevos Zero-Days explotados en su tecnología

Apple ha abordado tres nuevas vulnerabilidades explotadas en ataques activos contra iPhones, Macs y iPads.

Todos los errores de seguridad se encuentran en el motor de navegador WebKit multiplataforma y se rastrean como CVE-2023-32409, CVE-2023-28204 y CVE-2023-32373.

Prioridad: 1 Crítico.

Ampliar información:

- https://support.apple.com/en-us/HT213757
- https://www.bleepingcomputer.com/news/apple/apple-fixes-three-new-zero-days-exploited-to-hack-iphones-macs/

Vulnerabilidad en Keepass permite obtener contraseña maestra mediante volcado de memoria RAM

El investigador de seguridad "Vdhoney" describió la vulnerabilidad como una que solo un atacante con acceso de lectura al sistema de archivos o RAM del host podría explotar. Además, señaló que la vulnerabilidad tiene que ver con la forma en que un cuadro personalizado de KeePass, llamado "***SecureTextBoxEx***" *(sic),* permite ingresar contraseñas.

Prioridad: 1 Crítica.

Ampliar información:

- https://www.darkreading.com/application-security/keepass-vulnerability-imperils-master-passwords
- https://blog.segu-info.com.ar/2023/05/vulnerabilidad-en-keepass-permite.html

---

Microsoft tardará casi un año en terminar de parchear un nuevo error de arranque seguro

Esta semana, Microsoft publicó un parche para corregir un error de bypass de Secure Boot utilizado por el bootkit BlackLotus del que informamos en marzo. La vulnerabilidad original, CVE-2022-21894, fue parcheada en enero, pero el nuevo parche para CVE-2023-24932 aborda otra solución explotada activamente para sistemas que ejecutan Windows 10 y 11 junto con versiones de Windows Server que se remontan a Windows Server 2008.

Prioridad: 1 Crítica.

Ampliar información:

https://arstechnica.com/information-technology/2023/05/microsoft-patches-secure-boot-flaw-but-wont-enable-fix-by-default-until-early-2024/

Actualización de seguridad 6.2.1 para WordPress

Esta actualización menor incluye 20 correcciones a fallos en el núcleo y 10 correcciones de fallos en el editor de bloques. También incluye varias correcciones de seguridad, con una actualización desde WordPress 4.1.

Prioridad: 1 Crítica.

Ampliar información:

https://www.incibe.es/incibe-cert/alerta-temprana/avisos/actualizacion-de-seguridad-621-para-wordpress
https://es.wordpress.org/2023/05/16/wordpress-6-2-1-actualizacion-de-mantenimiento-y-seguridad/

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y/o aplicaciones actualizadas.
- Realizar actualizaciones directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se puede realizar la actualización inmediatamente, dichos controles pueden incluir controles tecnológicos y soluciones de seguridad avanzadas que le permitan minimizar el riesgo de que alguna vulnerabilidad sea explotada.

- Tener una política y un plan de mitigación de vulnerabilidades periódico.
- Contar con soluciones de gestión de vulnerabilidades que le permita hacer la priorización de estas.
- Adquirir tecnologías que le permitan bloquear accesos mal intencionados o intentos de explotación de vulnerabilidades conocidas y de día cero.
- Contar con servicios de Ethical Hacking para identificar posibles superficies de ciberataque antes de que lo hagan sus adversarios, protegiendo los datos sensibles de un uso indebido o de robo, ayudando a prevenir las amenazas en la seguridad de los datos e identificar las vulnerabilidades que pueden ir más allá del sistema perimetral, con el fin de establecer un análisis holístico de las amenazas que puedan comprometer la seguridad de los datos críticos de la compañía, entre otras.

MALWARE

El alza de técnicas de ingeniería social y funcionalidades maliciosas genera un aumento de descargas de malware

Netskope, líder en Secure Access Service Edge (SASE), presenta una nueva investigación que confirma que los atacantes están encontrando nuevas formas de evadir la detección y camuflarse con el tráfico de red normal, utilizando HTTP y HTTPS para distribuir malware. Así, en su último Informe sobre Nube y Amenazas: Global Cloud and Web Malware Trends, Netskope identificó que, en promedio, cinco de cada 1.000 usuarios empresariales intentaron descargar malware en el primer trimestre de 2023, y las nuevas familias y variantes de malware representaron el 72% de dichas descargas.

Prioridad: 3 Importante.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/05/21/el-alza-de-las-tecnicas-de-ingenieria-social-y-las-funcionalidades-maliciosas-genera-un-gran-aumento-de-descargas-de-malware/

- https://www.netskope.com/resources/reports-guides/cloud-and-threat-report-global-cloud-and-web-malware-trends

- https://finance.yahoo.com/news/netskope-attackers-double-down-social-040100740.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAALvFXfgACiI7bWhrZ7FxEvk-m1dQcUugKR93_RsWfLNpSC5M9y0DnVNCLGieKGCSuclMCDVOx3HaGp42JqDiAbFbc7x9Lf7zpFId9H5J2FdEzn8zLkDjRsxe0aH91Y1xtk8Ghvht-WeA7HcsBfyJHvdob07UyCZkC7Anllrq3lcz#:~:text=In%20its%20latest%20Cloud%20%26%20Threat,72%25%20of%20those%20malware%20downloads.

El ransomware MalasLocker se dirige a los servidores de Zimbra y exige una donación benéfica

Una nueva operación de ransomware está hackeando servidores Zimbra para robar correos electrónicos y cifrar archivos. Sin embargo, en lugar de exigir el pago de un rescate, los actores de amenazas afirman que requieren una donación a la caridad para proporcionar un cifrador y evitar la fuga de datos.

Prioridad: 3 Importante.

Ampliar información:

- https://blog.segu-info.com.ar/2023/05/malaslocker-nuevo-ransomware-activo.html

https://www.bleepingcomputer.com/news/security/malaslocker-ransomware-targets-zimbra-servers-demands-charity-donation/

Descubren una campaña masiva de malware precargado para Android

Investigadores de Trend Micro han descubierto una campaña masiva de ciberdelincuencia que ha infectado casi 9 millones de dispositivos basados en Android con malware precargado.

Prioridad: 3 Importante.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/05/20/descubren-una-campana-masiva-de-malware-precargado-para-android-que-afecta-a-millones-de-personas/

Recomendaciones generales sobre Malware:

- Controlar de forma minuciosa las conexiones de acceso remoto a su infraestructura: prohíba las conexiones desde redes públicas, permita el acceso RDP solo mediante un canal VPN y use contraseñas seguras y únicas con la autenticación en dos pasos.
- Mantener actualizado el software crítico de manera oportuna, poniendo énfasis en el sistema operativo, las soluciones de seguridad, los clientes de VPN y las herramientas de acceso remoto.
- Mantener a sus empleados constantemente en capacitaciones de concientización de ciberseguridad y en programas de sensibilización de ciberseguridad. En Gamma Ingenieros contamos con un programa completo de sensibilización en

ciberseguridad, para obtener más información contacte a su gerente de cuenta, preguntando por nuestro programa de sensibilización y nuestra plataforma propietaria, Gamma Cyberacademy ©.

- Emplear soluciones de ciberseguridad avanzadas para proteger los dispositivos de trabajo y el perímetro de la red corporativa.
- Mantener actualizadas sus soluciones de ciberseguridad.
- Descargar aplicaciones solo de fuentes de confianza, como la tienda oficial de aplicaciones de Google Play Store.
- Revisar las calificaciones y opiniones de otras personas antes de descargar cualquier aplicación, especialmente si es una aplicación bancaria o financiera.
- No responder a llamadas telefónicas de números desconocidos o sospechosos, especialmente si solicitan información personal o financiera.
- No compartir información personal o financiera a través del teléfono o correo electrónico, a menos que esté seguro de la identidad del destinatario.

BRECHAS DE SEGURIDAD

Toyota admite una fuga de datos de una década que afecta a 2,15 millones de clientes

Toyota Motor Corp ha reconocido que los datos de los vehículos de aproximadamente 2,15 millones de usuarios estuvieron accesibles públicamente en Japón durante casi una década, desde noviembre de 2013 hasta mediados de abril de 2023.

Prioridad: 1 Crítica

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/05/13/toyota-admite-una-fuga-de-datos-de-una-decada-que-afecta-a-215-millones-de-clientes/
- https://www.bleepingcomputer.com/news/security/toyota-car-location-data-of-2-million-customers-exposed-for-ten-years/

NOTICIAS DE CIBERSEGURIDAD

Gartner identifica seis riesgos de ChatGPT que los líderes legales y de cumplimiento deben evaluar

Los líderes legales y de cumplimiento enfrentan la responsabilidad de evaluar los riesgos asociados con ChatGPT y establecer medidas adecuadas para un uso responsable de estas herramientas de inteligencia artificial generativa.
Gartner, Inc., una reconocida firma de investigación y consultoría, ha identificado seis riesgos críticos que los líderes legales y de cumplimiento deben abordar al utilizar ChatGPT y otras herramientas de modelo de lenguaje (LLM) similares. Estos riesgos pueden exponer a las organizaciones a consecuencias legales, de reputación y financieras si no se toman las precauciones adecuadas.

Prioridad: 3 Importante.

Ampliar información:

- https://www.gartner.com/en/newsroom/press-releases/2023-05-18-gartner-identifies-six-chatgpt-risks-legal-and-compliance-must-evaluate?s=09&_its=JTdCJTIydmlkJTIyJTNBJTIyNTQ4OTMzOWEtMWU1Yy00NWY5LWJkOGUtY2Q4MWRhYjIxOTI4JTIyJTJDJTIyc3RhdGUlMjIlM0ElMjJybHR%2BMTY4NDY5NTE4OX5sYW5kfjJfMTY0NjZfdnJlZl80YzdmNGUwOTBkNmZlYTFmNWI5NjZkMDNhMDBjOWNkYyUyMiUyQyUyMnNpdGVJZCUyMiUzQTQwMTMxJTdE

Superintendencia de Industria y Comercio de Colombia investiga aplicación ChatGPT por protección de datos personales

La Superintendencia de Industria y Comercio (SIC), autoridad nacional de protección de datos personales de Colombia, ha iniciado una investigación sobre la aplicación ChatGPT para determinar si cumple con la regulación colombiana de protección de datos personales. La investigación se enmarca en un trabajo conjunto de la Red Iberoamericana de Protección de Datos, que involucra a otras 15 autoridades de la región.

Prioridad: 3 Importante.

Ampliar información:

- https://www.sic.gov.co/slider/superindustria-le-pone-la-lupa-la-aplicacion-chat-gpt-para-determinar-si-cumple-con-la-regulacion-de-proteccion-de-datos-personales
- https://www.portafolio.co/economia/gobierno/chatgpt-sic-investigara-si-la-herramienta-cumple-con-regulacion-de-proteccion-de-datos-582850

Microsoft advierte sobre aumento de ataques que comprometen el correo electrónico de las empresas

Microsoft ha publicado un nuevo informe en el que advierte a las empresas sobre el alarmante aumento de los ataques contra el correo electrónico empresarial (BEC) y la evolución de las tácticas empleadas por los ciberdelincuentes.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/05/20/microsoft-advierte-del-aumento-de-los-ataques-que-comprometen-el-correo-electronico-de-las-empresas/