GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2224

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	0	1	8
MALWARE	0	1	4
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Vulnerabilidad CVE-2024-34359 en paquete de Python cpp_python en modelos de IA

La vulnerabilidad crítica CVE-2024-34359 afecta al paquete llama_cpp_python, utilizado para integrar modelos de IA con Python. Si se explota, permite a los atacantes ejecutar código arbitrario en el sistema, comprometiendo datos y operaciones. El riesgo surge al descargar un modelo de IA aparentemente seguro desde plataformas confiables como Hugging Face, que podría abrir una puerta trasera para el control del sistema por parte de los atacantes.

Prioridad: 2 Urgente.

Ampliar información:

https://www.securityweek.com/critical-flaw-in-ai-python-package-can-lead-to-system-and-data-compromise

---

Microsoft aun no ha parcheado vulnerabilidades de día cero

Microsoft lanzó una extensa serie de correcciones de seguridad durante su última actualización de Patch Tuesday, abordando alrededor de cinco docenas de problemas, entre ellos las vulnerabilidades CVE-2024-30051 y CVE-2024-30040 que están siendo activamente explotadas. Sin embargo, a diferencia de sus contrapartes, Apple y Google, Microsoft aún no ha solucionado varias vulnerabilidades identificadas por investigadores en marzo. Hasta ahora, solo han abordado una de estas vulnerabilidades, la cual también afectaba a Google Chrome y fue resuelta por Google, con Microsoft adaptándola a su navegador, Edge.

Las vulnerabilidades no parchadas pueden permitir fuga de datos, comprometer sistemas con malware y causar interrupciones en servicios críticos. También pueden facilitar el compromiso del sistema.

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/vulnerabilities-threats/microsoft-has-yet-to-patch-7-pwn2own-zero-days

---

Explotación de Vulnerabilidad CVE-2024-22026 en MobileIron Core

Ivanti EPMM, anteriormente MobileIron Core, presenta la vulnerabilidad de alta gravedad CVE-2024-22026, que permite la escalada de privilegios locales a través de un comando

en el shell restringido clish. La vulnerabilidad afecta a versiones anteriores a 12.1.0.0, 12.0.0.0 y 11.12.0.1, y ha sido solucionada con las últimas actualizaciones de Ivanti.

Prioridad: 3 Importante.

Ampliar información:

https://www.redlinecybersecurity.com/blog/exploiting-cve-2024-22026-rooting-ivanti-epmm-mobileiron-core

---

Vulnerabilidad CVE-2024-4323 crítica en Fluent Bit afecta plataformas en la nube

Tenable ha descubierto una vulnerabilidad crítica (CVE-2024-4323) en Fluent Bit, una utilidad de registro utilizada por importantes proveedores de servicios en la nube y compañías tecnológicas. Esta vulnerabilidad, apodada "Linguistic Lumberjack", es un desbordamiento de búfer en el servidor HTTP integrado en Fluent Bit, lo que podría permitir ataques de denegación de servicio.

Prioridad: 3 Importante.

Ampliar información:

https://www.helpnetsecurity.com/2024/05/21/cve-2024-4323/

GitHub alerta sobre fallo de bypass de autenticación SAML en su servidor empresarial

GitHub ha corregido una vulnerabilidad crítica de bypass de autenticación (CVSS v4 score: 10.0), identificada como CVE-2024-4985, que afecta a las instancias del Servidor Empresarial de GitHub (GHES), las cuales, utilizan autenticación SAML de inicio de sesión único (SSO). Esta vulnerabilidad permitiría a un actor malintencionado falsificar una

respuesta SAML y obtener privilegios de administrador, lo que proporcionaría acceso sin restricciones a todo el contenido de la instancia sin necesidad de autenticación.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/05/critical-github-enterprise-server-flaw.html

---

Vulnerabilidad critica en Netflix Genie expone Big Data

Se ha descubierto una vulnerabilidad crítica en la versión de código abierto del motor de orquestación de trabajos Genie de Netflix. Esta vulnerabilidad, designada como CVE-2024-4701, permite a atacantes remotos ejecutar código arbitrario en sistemas afectados. La puntuación de gravedad asignada es de 9.9 en la escala CVSS, lo que la considera de alta importancia. La vulnerabilidad afecta a organizaciones que gestionan su propia instancia de Genie OSS, utilizando el sistema de archivos local para cargar y almacenar archivos adjuntos de usuarios.

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/application-security/netflix-fixes-critical-vulnerability-on-big-data-orchestration-service

---

Vulnerabilidades criticas de inyección SQL afectan al administrado de puentos finales de Ivanti

Ivanti ha solucionado varios fallos en su Administrador de Puntos Finales (EPM), incluyendo vulnerabilidades de ejecución remota de código. Ivanti lanzó parches de seguridad para abordar múltiples vulnerabilidades críticas en el EPM. Estas vulnerabilidades podrían ser

explotadas por atacantes remotos para ejecutar código en el sistema, bajo ciertas condiciones. Los fallos afectan a las versiones 2022 SU5 y anteriores. Seis de las 10 vulnerabilidades (CVE-2024-29822, CVE-2024-29823, CVE-2024-29824, CVE-2024-29825, CVE-2024-29826, CVE-2024-29827) han sido clasificadas como críticas, con una puntuación CVSS de 9.6.

Prioridad: 3 Importante.

Ampliar información:

https://securityaffairs.com/163587/security/ivanti-endpoint-manager-critical-sql-injection.html

---

Vulnerabilidad y Exploit en Foxit PDF Reader en versión 2024.3.

Los actores de múltiples amenazas están aprovechando una falla de diseño en el lector de PDF Foxit para distribuir una variedad de malware, incluyendo Agente Tesla, Asyncrat, DCRAT, Nanocore Rat, NJRAT, Pony, REMCOS RAT y XWORM. Este exploit desencadena advertencias de seguridad que podrían engañar a los usuarios para ejecutar comandos dañinos, según un informe técnico de Check Point.

Prioridad: 3 Importante.

Ampliar información:

https://blog.segu-info.com.ar/2024/05/vulnerabilidad-y-exploit-en-foxit-pdf.html?utm_source=SeguInfo&utm_medium=SeguInfo&utm_campaign=Segu-Info%20-%20Ciberseguridad%20desde%20el%202000&utm_content=Segu-Info%20-%20Ciberseguridad%20desde%20el%202000&lctg=205608146

Vulnerabilidad crítica de RCE no autenticada en Fortinet FortiSIEM versiones 6.4.0 a 7.1.1.

Investigadores de Horizon3.ai descubrieron una vulnerabilidad crítica de ejecución remota de código no autenticada en Fortinet FortiSIEM, identificada como CVE-2023-34992. Esta vulnerabilidad, con una puntuación CVSS de 10,0, ha sido explotada mediante un exploit de prueba de concepto (PoC). FortiSIEM es una solución integral de gestión de eventos e información de seguridad (SIEM) que ofrece capacidades de recopilación de registros, correlación, respuesta automatizada y corrección.

Prioridad: 3 Importante.

Ampliar información:

https://cybersecuritynews.com/rce-vulnerability-fortinet-fortisiem/

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

Campaña de publicidad maliciosa que contiene ransomware

Rapid7 ha detectado una campaña continua que distribuye instaladores troyanizados de WinSCP y PuTTY mediante anuncios maliciosos en motores de búsqueda populares. Estos anuncios redirigen a los usuarios a dominios con errores tipográficos. En al menos un caso, la infección resultante ha intentado desplegar ransomware.

Prioridad: 3 Importante.

Ampliar información:

https://www.rapid7.com/blog/post/2024/05/13/ongoing-malvertising-campaign-leads-to-ransomware/

Ciberdelincuentes explotan GitHub y FileZilla para distribuir malware Cocktail

Una campaña de ciberataques está utilizando servicios legítimos como GitHub y FileZilla para distribuir una variedad de malware tipo “Stelaler” y troyanos bancarios, haciéndose pasar por software confiable como Password y Pixelmator Pro. Esta actividad, conocida como GitCaught, muestra cómo se están utilizando múltiples variantes de malware para atacar dispositivos Android, macOS y Windows. Los atacantes crean perfiles y repositorios falsos en GitHub para alojar versiones falsificadas de software, con el objetivo de robar datos sensibles de dispositivos comprometidos.

Prioridad: 3 importante.

Ampliar información:

https://thehackernews.com/2024/05/cyber-criminals-exploit-github-and.html

---

Void Manticore la colaboración estructurada entre espionaje y destrucción en MOIS

Check Point Research (CPR) ha estado siguiendo de cerca las acciones de Void Manticore, un actor de amenazas iraní vinculado al Ministerio de Inteligencia y Seguridad (MOIS). Este grupo ha destacado por su participación en ataques de borrado destructivo, a menudo combinados con operaciones de influencia. Lo notable es que Void Manticore ha adoptado múltiples identidades en línea para llevar a cabo sus operaciones, siendo las más destacadas "Homeland Justice" para ataques en Albania y "Karma" para operaciones dirigidas a Israel.

Prioridad: 3 Importante.

Ampliar información:

https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel/

El aumento de los Stealers, una amenaza creciente en ciberseguridad

Los “Stealers” son una amenaza importante en el mundo del malware. En el último año, se han identificado y estudiado varios de estos programas maliciosos. Recientemente, se han descubierto nuevos 'stealers' como Acrid y ScarletStealer, así como actualizaciones en los “stealers” existentes como Sys01.

Prioridad: 3 Importante.

Ampliar información:

https://securelist.com/crimeware-report-stealers/112633/

Keylogger en Microsoft Exchange Server

El Centro de Seguridad de Expertos (PT ESC) de Positive Technologies descubrió un sofisticado keylogger oculto en la página principal de los Servidores de Microsoft Exchange. Se trata de una violación de seguridad importante que afecta a empresas y organismos gubernamentales en todo el mundo.

Prioridad: 2 Urgente.

Ampliar información:

https://cybersecuritynews.com/keylogger-embedded-microsoft-exchange-server/

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

Los ciberdelincuentes cambian de táctica para presionar a más víctimas a pagar rescates

En 2023, el ransomware experimentó un crecimiento y evolución significativos en los Estados Unidos, según datos de At-Bay. La frecuencia de los reclamos de ransomware aumentó un 64% respecto al año anterior, impulsada principalmente por un incremento del 415% en incidentes "indirectos" de ransomware.

Prioridad: 3 Importante.

Ampliar información:

https://www.helpnetsecurity.com/2024/05/20/ransomware-claims-frequency-grow/

Desmantelamiento de Lockbit cambia el panorama de los grupos de Ransomware líderes

Después de la desarticulación de LockBit en febrero, el grupo rival Play ha superado a LockBit en número de ataques, marcando un cambio en el panorama de los grupos de ransomware. Este cambio sugiere que las acciones de las fuerzas del orden para interrumpir las operaciones de LockBit han tenido éxito. La revelación de la identidad del presunto líder de LockBit y la actualización de la Agencia Nacional contra el Crimen indican que la capacidad operativa de LockBit se ha visto reducida significativamente.

Prioridad: 3 Importante.

Ampliar información:

https://www.theregister.com/2024/05/22/lockbit_dethroned_as_leading_ransomware/