GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0825

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

VULNERABILIDADES

Atlassian evalua vulnerabilidades críticas en Confluence y Crowd

Atlassian ha lanzado actualizaciones de seguridad para abordar 12 vulnerabilidades de severidad crítica y alta en sus productos Bamboo, Bitbucket, Confluence, Crowd y Jira. En particular, se han corregido cinco fallos críticos en Confluence Data Center y Server, así como en Crowd Data Center y Server, los cuales fueron descubiertos en dependencias de terceros utilizadas en estos productos. Dos de estas vulnerabilidades, identificadas como CVE-2024-50379 y CVE-2024-56337, afectan a Apache Tomcat y podrían ser explotadas por atacantes no autenticados para ejecutar código de forma remota. Además, una tercera vulnerabilidad crítica en Apache Tomcat, CVE-2024-52316, podría permitir la omisión de autenticación en Crowd.

Para mitigar estos riesgos, Atlassian recomienda a los usuarios actualizar sus instalaciones a las versiones más recientes de los productos afectados lo antes posible. Aunque la

compañía no ha reportado explotación activa de estas vulnerabilidades, es crucial aplicar los parches disponibles para garantizar la seguridad de los sistemas. Las actualizaciones también abordan otras vulnerabilidades de alta severidad, incluyendo fallos de denegación de servicio en Bamboo y Jira, y una vulnerabilidad de ejecución remota de código en Bitbucket.

Prioridad: Importante.

Ampliar Información:

https://www.securityweek.com/atlassian-patches-critical-vulnerabilities-in-confluence-crowd/

Microsoft soluciona vulnerabilidad de zero-day en Power Pages explotada en ataques

Microsoft ha abordado una vulnerabilidad de alta severidad en Power Pages, identificada como CVE-2025-24989, que permitía a actores no autorizados elevar sus privilegios a través de la red y eludir los controles de registro de usuarios. Esta falla de control de acceso inapropiado fue explotada como un zero-day en ataques recientes. Power Pages es una plataforma de desarrollo web de bajo código que forma parte de Microsoft Power Platform, utilizada para crear y gestionar sitios web empresariales orientados al público.

Para mitigar este problema, Microsoft ha implementado soluciones a nivel de servicio y ha notificado a los clientes afectados, proporcionando instrucciones para detectar posibles compromisos. La compañía ha declarado: "Esta vulnerabilidad ya ha sido mitigada en el servicio y todos los clientes afectados han sido notificados". Se recomienda a los usuarios de Power Pages revisar sus sitios en busca de signos de explotación y seguir las directrices proporcionadas por Microsoft para garantizar la seguridad de sus implementaciones.

Prioridad: Urgente.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/microsoft-fixes-power-pages-zero-day-bug-exploited-in-attacks/

CISA advierte sobre vulnerabilidad crítica en Craft CMS

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha añadido la vulnerabilidad CVE-2025-23209 a su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), esto debido a evidencia de explotación activa. Esta vulnerabilidad afecta a las versiones 4 y 5 de Craft CMS, un sistema de gestión de contenido ampliamente utilizado. Los administradores del proyecto abordaron este problema en diciembre de 2024 con las versiones 4.13.8 y 5.5.8. La falla permite la inyección de código que puede conducir a la ejecución remota del mismo, especialmente en versiones vulnerables que tienen claves de seguridad de usuario comprometidas.

Se recomienda encarecidamente a las empresas y usuarios que actualicen Craft CMS a las versiones parcheadas mencionadas. Si la actualización inmediata no es posible, se aconseja rotar la clave de seguridad y garantizar su privacidad para mitigar el riesgo. CISA ha establecido el 13 de marzo de 2025 como fecha límite para que los encargados de estas apliquen las correcciones necesarias. Además, en diciembre de 2024, Craft CMS advirtió sobre otra vulnerabilidad (CVE-2024-56145) que también podría permitir la ejecución remota de código cuando la configuración register_argc_argv de PHP está habilitada.

Prioridad: Urgente.

Ampliar Información:

https://thehackernews.com/2025/02/cisa-flags-craft-cms-vulnerability-cve.htmlvvvv

---

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

Malware Android Spylend: Más de 100.000 descargas en Google Play

Un reciente informe de BleepingComputer revela que el malware Android conocido como Spylend ha sido descargado más de 100.000 veces desde la tienda oficial de Google Play. Este software malicioso se propaga a través de aplicaciones que, a simple vista, parecen legítimas, lo que le permite infiltrarse en dispositivos móviles sin levantar sospechas. Aunque los detalles precisos sobre el actor implicado aún no se han revelado en profundidad, se sabe que detrás de esta campaña se encuentra un grupo de ciberdelincuentes con habilidades para disfrazar aplicaciones maliciosas de utilidades comunes. El descubrimiento del malware fue realizado por el equipo de investigadores de BleepingComputer, quienes alertaron sobre los riesgos que representa para la seguridad de los usuarios.

El malware Spylend está diseñado para operar de manera encubierta, recopilando información sensible del dispositivo, como datos personales, registros de llamadas y mensajes, y enviándolos a servidores controlados por los atacantes. Se trata de un software

sofisticado que logra evadir muchos de los mecanismos de detección habituales, lo que incrementa su peligrosidad. Entre las recomendaciones para los usuarios se destaca la necesidad de eliminar cualquier aplicación sospechosa, revisar cuidadosamente los permisos solicitados por las apps, y descargar únicamente aquellas desarrolladas por fuentes confiables, incluso cuando se trate de la Google Play Store. Estas medidas ayudarán a reducir el riesgo de infección y a proteger la información personal ante amenazas emergentes.

Prioridad: Urgente.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/spylend-android-malware-downloaded-100-000-times-from-google-play/

Cibercriminales utilizan Eclipse Jarsigner para desplegar malware XLoader

Una reciente campaña maliciosa, identificada por el AhnLab Security Intelligence Center, revela que cibercriminales están aprovechando la herramienta legítima jarsigner de la Eclipse Foundation para propagar el malware XLoader. Los atacantes empaquetan un archivo ZIP comprimido que incluye una versión renombrada del ejecutable original (Documents2012.exe), junto con bibliotecas DLL manipuladas—en particular, un "jli.dll" alterado que desencadena la carga del payload cifrado en "concrt140e.dll". Al ejecutar este archivo, se activa una técnica de DLL side-loading que inyecta el malware en procesos legítimos, facilitando la evasión de detección mediante la mezcla de tráfico legítimo y comunicaciones cifradas de comando y control.

XLoader, sucesor del malware Formbook y distribuido bajo un modelo de Malware-as-a-Service, se caracteriza por robar información sensible del sistema, como detalles del PC y del navegador, y por descargar malware adicional. Según el informe de Zscaler ThreatLabz, las versiones recientes (6 y 7) incorporan capas avanzadas de ofuscación y cifrado, lo que

dificulta su análisis y detección basada en firmas. Como recomendación, se aconseja a los usuarios y organizaciones extremar la precaución al abrir archivos ZIP sospechosos, verificar la integridad de los ejecutables y mantener actualizadas las soluciones de seguridad para mitigar riesgos derivados del abuso de aplicaciones legítimas.

Prioridad: Urgente.

Ampliar Información:

https://thehackernews.com/2025/02/cybercriminals-use-eclipse-jarsigner-to.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.

NOTICIAS DE CIBERSEGURIDAD

Microsoft y el DOJ desmantelan dominios de grupo hacker

En una operación coordinada, Microsoft y el Departamento de Justicia de EE. UU. han desmantelado una serie de dominios que eran utilizados por un grupo de hackers vinculado al FSB ruso. Este grupo, implicado en actividades cibernéticas maliciosas como ataques de phishing y ciber espionaje, aprovechaba estos dominios para llevar a cabo sus operaciones. La acción, llevada a cabo en el marco de un esfuerzo global contra el cibercrimen, evidencia la amenaza que representan actores estatales en el entorno digital.

El actor implicado, un grupo de hackers relacionado con el FSB, fue identificado gracias al trabajo conjunto de inteligencia realizado por Microsoft, en colaboración estrecha con el Departamento de Justicia. Como recomendación, se llama a las organizaciones a reforzar sus medidas de ciberseguridad: actualizar sus sistemas, implementar herramientas avanzadas de detección y respuesta ante incidentes, y revisar las políticas de acceso a redes para mitigar riesgos futuros.

Prioridad: Importante.

Ampliar Información:

https://www.securityweek.com/microsoft-doj-dismantle-domains-used-by-russian-fsb-linked-hacking-group/

OpenAI prohíbe cuentas que abusan de ChatGPT para vigilancia e influencia

OpenAI anunció la eliminación de un grupo de cuentas que abusaban de su herramienta ChatGPT para desarrollar una supuesta herramienta de vigilancia con capacidades de inteligencia artificial. Estas cuentas, de presunto origen chino y apoyadas en modelos como Llama de Meta, emplearon ChatGPT para generar descripciones detalladas y analizar documentos, con el objetivo de recolectar datos en tiempo real sobre protestas anti-China

en Occidente. La campaña, denominada “Peer Review”, fue identificada por los investigadores Ben Nimmo, Albert Zhang, Matthew Richard y Nathaniel Hartley, quienes detectaron que incluso se utilizaba ChatGPT para depurar y modificar el código fuente del software denominado "Qianyue Overseas Public Opinion AI Assistant".

La acción se enmarca en un contexto de creciente uso de herramientas de IA por actores maliciosos para facilitar campañas de desinformación, espionaje y manipulación de opinión pública. Ante esta situación, se recomienda a las empresas tecnológicas y plataformas de redes sociales fortalecer sus mecanismos de monitoreo y colaborar estrechamente con proveedores y organismos reguladores para detectar y neutralizar actividades sospechosas. Además, es fundamental que la comunidad de ciberseguridad comparta sus hallazgos y alertas para prevenir el uso indebido de estas tecnologías y proteger la integridad de la información en la era digital.

Prioridad: Importante.

Ampliar Información:

https://www.securityweek.com/apple-confirms-usb-restricted-mode-exploited-in-extremely-sophisticated-attack/