GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

En alianza con

TD SYNNEX FORTINET

Edición °3524

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

VULNERABILIDADES

Vulnerabilidades en Progress WhatsUp Gold permiten la inyección de comandos SQL

Progress ha confirmado la existencia de vulnerabilidades críticas en todas las versiones de WhatsUp Gold anteriores a la 2024.0.0, que podrían permitir a atacantes inyectar comandos SQL y acceder a contraseñas encriptadas. Estas vulnerabilidades, identificadas como CVE-2024-6670, CVE-2024-6671 y CVE-2024-6672, son altamente peligrosas y se insta a los usuarios a actualizar a la última versión de inmediato para mitigar los riesgos de seguridad.

Prioridad: 1 Crítico.

Ampliar información:

https://gbhackers.com/progress-whatsup-gold-vulnerabilities

Falla crítica de autenticación afecta a GitHub Enterprise Server

GitHub ha lanzado una actualización urgente para corregir tres defectos de seguridad en GitHub Enterprise Server, advirtiendo que uno de ellos, identificado como CVE-2024-6800, podría permitir a los atacantes obtener privilegios de administrador del sitio. Esta vulnerabilidad, con una puntuación CVSS de 9.5/10, afecta a la autenticación SAML SSO y ha sido corregida en las versiones 3.13.3, 3.12.8, 3.11.14 y 3.10.16 de GitHub Enterprise Server. Se recomienda a los usuarios corporativos aplicar la actualización de inmediato.

Prioridad: 2 Urgente.

Ampliar información:

https://www.securityweek.com/critical-authentication-flaw-haunts-github-enterprise-server/

Vulnerabilidad en plugin de caché instalado en 5 millones de sitios de WordPress

Una vulnerabilidad crítica en el plugin Litespeed Cache de WordPress podría permitir a atacantes tomar control de millones de sitios al crear un usuario administrador. Descubierta en agosto de 2024 y rastreada como CVE-2024-28000, esta falla permite a un atacante no autenticado escalar privilegios y obtener acceso de administrador. Aunque el parche fue lanzado el 13 de agosto, muchos sitios siguen siendo vulnerables. La explotación de esta vulnerabilidad es altamente probable, especialmente en ataques dirigidos.

Prioridad: 1 Crítico.

Ampliar información:

https://www.securityweek.com/exploitation-expected-for-flaw-in-caching-plugin-installed-on-5m-wordpress-sites/

Vulnerabilidad crítica en Microsoft Copilot Studio expone datos sensibles

Investigadores de ciberseguridad han revelado una vulnerabilidad crítica en Microsoft Copilot Studio, identificada como CVE-2024-38206 con una puntuación CVSS de 8.5. Este fallo, causado por un ataque de Server-Side Request Forgery (SSRF), permite a un atacante autenticado acceder a información sensible a través de solicitudes web externas. Aunque Microsoft ya solucionó el problema sin requerir acción por parte de los usuarios, la vulnerabilidad expone la infraestructura interna de Copilot Studio, lo que podría afectar a múltiples clientes.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/08/microsoft-patches-critical-copilot.html?&web_view=true

---

Nueva vulnerabilidad crítica en SolarWinds Web Help Desk (CVE-2024-28987)

SolarWinds ha lanzado una nueva corrección para una vulnerabilidad crítica en Web Help Desk (WHD) identificada como CVE-2024-28987, apenas una semana después de solucionar otro defecto crítico (CVE-2024-28986). Esta nueva falla se debe a credenciales codificadas en el software que pueden ser explotadas por usuarios remotos no autenticados para acceder a funciones internas y modificar datos. Reportada por el investigador de vulnerabilidades Zach Hanley de Horizon3.ai, la vulnerabilidad permite a los atacantes acceder al sistema sin autenticación previa. La corrección, incluida en el Hotfix 2 de Web Help Desk 12.8.3, también aborda el problema previo y otros errores, por lo cual se recomienda a los administradores implementar esta actualización de inmediato para asegurar la protección del sistema.

Prioridad: 1 Crítico.

Ampliar información:

https://www.helpnetsecurity.com/2024/08/23/cve-2024-28987/?web_view=true

---

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

La vulnerabilidad de Log4j se explota nuevamente para ataques de criptominería

La conocida vulnerabilidad de Log4j, también llamada Log4Shell, está siendo explotada nuevamente, esta vez para desplegar malware de criptominería. Los ataques recientes implican el envío de solicitudes LDAP ofuscadas que desencadenan la ejecución de scripts maliciosos, lo que permite a los atacantes obtener control del sistema, establecer persistencia y exfiltrar datos. Los atacantes aprovechan la falla de Log4Shell para instalar XMRig, un software de criptominería en sistemas comprometidos, lo que demuestra los riesgos continuos que plantea esta vulnerabilidad. La persistencia del ataque y su capacidad para evadir la detección subrayan la necesidad crítica de mantenerse alerta ante las amenazas relacionadas con Log4j.

Prioridad: 3 Importante.

Ampliar información:

https://gbhackers.com/log4j-exploited-crypto-mining/

Nuevo malware Cthulhu Stealer apunta a usuarios de macOS

El malware Cthulhu Stealer, descubierto por Cado Security, está diseñado para robar información en sistemas macOS. Este malware se distribuye a través de imágenes de disco de Apple (DMG) disfrazadas de software legítimo. Roba credenciales, información de criptomonedas y otros datos sensibles utilizando herramientas de línea de comandos de macOS. Aunque sus desarrolladores han sido expulsados de algunos mercados, Cthulhu Stealer destaca el creciente riesgo de ciberataques para los usuarios de macOS.

Prioridad: 3 Importante.

Ampliar información:

https://securityaffairs.com/167454/malware/cthulhu-stealer-targets-apple-macos.html

---

Ransomware Qilin roba credenciales almacenadas en Google Chrome

Un análisis reciente del ransomware Qilin por parte del equipo Sophos X-Ops reveló una táctica inusual: el robo masivo de credenciales almacenadas en navegadores Google Chrome. El ataque, ocurrido en julio de 2024, implicó el uso de scripts maliciosos en políticas de grupo para extraer contraseñas desde los navegadores de las máquinas afectadas. Qilin, conocido por ataques de "doble extorsión", ahora también explora el robo de datos de credenciales, exacerbando el impacto del ransomware al comprometer potencialmente numerosos sitios de terceros. Esta técnica añade una capa de complejidad a la respuesta y remediación de las brechas de seguridad.

Prioridad: 2 Urgente.

Ampliar información:

https://news.sophos.com/en-us/2024/08/22/qilin-ransomware-caught-stealing-credentials-stored-in-google-chrome/?web_view=true

---

Malware 'sedexp' para Linux evade detección durante dos años

El malware para Linux conocido como 'sedexp' ha evadido la detección desde 2022 utilizando una técnica de persistencia aún no documentada en el marco MITRE ATT&CK. Descubierto por la firma de gestión de riesgos Stroz Friedberg, 'sedexp' emplea reglas de udev para asegurar su persistencia, ejecutándose cada vez que se agrega un nuevo dispositivo al sistema. Esta técnica se basa en la manipulación de archivos de dispositivo, como /dev/random, que no son monitorizados por soluciones de seguridad, permitiendo al malware permanecer oculto. Además, 'sedexp' oculta sus archivos y procesos, para

establecer shells reversos en el acceso remoto, subrayando su sofisticación y capacidad para realizar ataques dirigidos, como el robo de datos financieros.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/stealthy-sedexp-linux-malware-evaded-detection-for-two-years/?&web_view=true

---

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

Hackers utilizan países del sur global como campo de pruebas para ciberataques

Los piratas informáticos han adoptado la estrategia de infiltrarse en sistemas informáticos en países del sur global como un método de prueba antes de dirigirse a objetivos más lucrativos en América del Norte y Europa. Este enfoque ha permitido a los hackers experimentar con sus tácticas en entornos con menor protección cibernética, como un banco en Senegal y empresas en Chile, Colombia y Argentina. Estas pruebas reflejan un aumento global de ciberataques, exacerbado por la rápida digitalización y la inadecuada ciberseguridad en países en desarrollo, dejando a sus sistemas vulnerables a futuras amenazas.

Prioridad: 3 Importante.

Ampliar información:

https://www.pandasecurity.com/es/mediacenter/hackers-utilizan-paises-emergentes-para-entrenar-ataques-de-ransomware/
