GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

En alianza con

TD SYNNEX FORTINET

Edición °3724

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

VULNERABILIDADES

Vulnerabilidad crítica en LiteSpeed Cache CVE-2024-44000

Un fallo crítico en el plugin LiteSpeed Cache, identificado como CVE-2024-44000, permite la toma de control de sitios WordPress sin autenticación. La vulnerabilidad se debe a que el plugin registra cookies de sesión en un archivo de depuración, que los atacantes pueden explotar para robar sesiones de administrador. Las versiones afectadas son anteriores a la 6.5.0.1, donde ya se ha lanzado un parche.

Se recomienda actualizar de inmediato a la versión 6.5.0.1, eliminar archivos "debug.log" y aplicar reglas .htaccess para proteger archivos de registro.

Prioridad: 1 Crítico.

Ampliar información:

https://www.bleepingcomputer.com/news/security/litespeed-cache-bug-exposes-6-million-wordpress-sites-to-takeover-attacks/

Vulnerabilidad de escalamiento de privilegios en Cisco ISE CVE-2024-20469 corregida.

Cisco ha corregido una vulnerabilidad de inyección de comandos en su plataforma Identity Services Engine (ISE). Esta vulnerabilidad, identificada como CVE-2024-20469, permite a atacantes con permisos de administrador escalar privilegios hasta nivel root, lo que podría comprometer considerablemente la seguridad del sistema.

Las versiones afectadas son ISE 3.2 y 3.3, las cuales ya cuentan con parches en las actualizaciones 3.2P7 y 3.3P4. Se recomienda a los usuarios actualizar de inmediato para prevenir posibles explotaciones, ya que se ha hecho pública una prueba de concepto del exploit.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/cisco-fixes-root-escalation-vulnerability-with-public-exploit-code/

Vulnerabilidad de escalamiento de privilegios en Android bajo explotación activa.

Google ha confirmado la explotación activa de la vulnerabilidad CVE-2024-32896 en el sistema operativo Android, que permite el escalamiento de privilegios locales a través de

un error lógico en el Framework de Android. Aunque inicialmente se creyó que afectaba solo a dispositivos Pixel, se ha confirmado que impacta a todo el ecosistema Android.

Google ya ha lanzado actualizaciones de seguridad para mitigar esta vulnerabilidad. Se recomienda actualizar los dispositivos Android a la versión más reciente disponible para evitar posibles ataques.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/09/google-confirms-cve-2024-32896.html

---

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 malware SpyAgent en Android roba frases de recuperación de criptomonedas

SpyAgent, un malware descubierto por McAfee, utiliza tecnología de reconocimiento óptico de caracteres (OCR) para robar frases de recuperación de criptomonedas a partir de imágenes guardadas en dispositivos Android. Inicialmente dirigido a Corea del Sur, este malware se está expandiendo a otros países como el Reino Unido, propagándose a través de APKs maliciosos distribuidos fuera de Google Play.

Se recomienda evitar fuentes no oficiales de apps, limitar permisos innecesarios y habilitar Google Play Protect para prevenir infecciones.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/spyagent-android-malware-steals-your-crypto-recovery-phrases-from-images/

Cibercriminales usan MacroPack para distribuir Havoc, Brute Ratel y PhantomCore

Investigadores de Cisco Talos descubrieron que atacantes están utilizando la herramienta MacroPack para distribuir malware avanzado como Havoc, Brute Ratel y PhantomCore. Estos malwares se están propagando a través de documentos maliciosos con macros, lo que permite a los atacantes ejecutar código y comprometer sistemas de forma remota.

Para mitigar riesgos, se recomienda deshabilitar macros en documentos no confiables, reforzar la detección de amenazas y monitorizar el uso de herramientas de red team en las redes.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/09/malware-attackers-using-macropack-to.html

---

Actores de amenaza norcoreanos distribuyen malware COVERTCATCH a través de estafas laborales en LinkedIn

Investigadores de Mandiant detectaron que actores de amenaza vinculados a Corea del Norte están utilizando campañas de ingeniería social en LinkedIn para distribuir el malware COVERTCATCH. Mediante falsos reclutamientos, los atacantes engañan a desarrolladores para que descarguen archivos ZIP maliciosos que contienen pruebas de código, comprometiendo principalmente sistemas macOS.

Se recomienda evitar interacciones con ofertas laborales sospechosas y escanear documentos y archivos de fuentes no confiables.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/09/north-korean-threat-actors-deploy.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

Pavel Durov critica leyes obsoletas tras su arresto por actividad criminal en Telegram

El CEO de Telegram, Pavel Durov, expresó su frustración por las leyes anticuadas tras su arresto en Francia, vinculado a delitos cometidos por terceros en la plataforma, como tráfico de drogas y lavado de dinero. Durov cuestiona que se culpe a los directivos por acciones de usuarios y resaltó que Telegram tiene más de 950 millones de usuarios activos. Telegram ha implementado medidas adicionales para reportar contenido ilegal y proteger a sus usuarios, pero Durov advierte que podrían retirarse de mercados que no respeten la privacidad de los usuarios.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/09/paul-durov-criticizes-outdated-laws.html

Grupo de espionaje TIDRONE apunta a fabricantes de drones en Taiwán

El grupo de espionaje TIDRONE, con posibles vínculos a actores de habla china, ha sido descubierto atacando fabricantes de drones en Taiwán. Según Trend Micro, la campaña cibernética iniciada en 2024 busca obtener información sensible del sector de defensa, utilizando malware personalizado como CXCLNT y CLNTEND a través de técnicas de control remoto.
Se sospecha de un ataque a la cadena de suministro, con herramientas diseñadas para escalar privilegios y evadir defensas de seguridad, lo que plantea graves riesgos para la industria militar.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/09/tidrone-espionage-group-targets-taiwan.html