

**GammaCSOC-CERT**  
By Gamma Ingenieros



# Boletín de Ciberseguridad Semanal

Edición °4124



## 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
<b>VULNERABILIDADES</b>	2	0	1
<b>MALWARE</b>	0	1	1
<b>NOTICIAS DE CIBERSEGURIDAD</b>	1		2

### VULNERABILIDADES

#### **Vulnerabilidad en el Plugin LiteSpeed Cache expone millones de sitios WordPress**

Un fallo de seguridad de alta severidad (CVE-2024-47374) fue descubierto en el plugin *LiteSpeed Cache*, usado en más de seis millones de sitios WordPress. Esta vulnerabilidad permite ataques de *cross-site scripting* (XSS) almacenado, donde un atacante no autenticado puede inyectar código malicioso en las páginas administrativas del sitio, afectando potencialmente su funcionamiento. El problema radica en la falta de sanitización en las funciones que manejan la generación de CSS, lo que permite que entradas maliciosas sean ejecutadas sin control. La vulnerabilidad puede derivar en el robo de información sensible o incluso en la toma de control total del sitio web si es explotada.

Para mitigar esta amenaza, se recomienda actualizar el plugin a la versión 6.5.1 o superior, que corrige el problema al implementar una sanitización adecuada de las entradas. Además, si no es posible realizar la actualización de inmediato, se sugiere desactivar las opciones "Combinar CSS" y "Generar UCSS" en la configuración de optimización de página, ya que estas funciones son necesarias para que el exploit tenga éxito.

**Prioridad:** 1 Crítico.

**Ampliar información:**

<https://thehackernews.com/2024/10/wordpress-litespeed-cache-plugin.html>

---

### **Exploit Crítico de Ejecución de Código en Ivanti Endpoint Manage**

Una vulnerabilidad crítica de Ejecución Remota de Código (RCE) en Ivanti Endpoint Manager (EPM), identificada como CVE-2024-29824, ha comenzado a ser explotada activamente por actores maliciosos. Esta falla, que afecta versiones anteriores a EPM 2022 SU5, permite a los atacantes ejecutar comandos arbitrarios en los sistemas afectados mediante inyección SQL. Investigadores de seguridad de Horizon3.ai publicaron un exploit de prueba de concepto (PoC) que facilita la explotación del fallo, lo que aumenta el riesgo de ataques. La vulnerabilidad se debe a una validación inadecuada de datos, lo que permite a los atacantes no autenticados acceder al servidor afectado.

Para mitigar este riesgo, se recomienda a los administradores aplicar inmediatamente las actualizaciones de seguridad publicadas por Ivanti en mayo de 2024. Además, se aconseja monitorear los logs de MS SQL para detectar cualquier uso anómalo de "xp\_cmdshell", que podría indicar intentos de explotación. La Agencia de Ciberseguridad y Seguridad de Infraestructuras de EE.UU. (CISA) ha ordenado a las agencias federales actualizar sus sistemas antes del 23 de octubre de 2024.

**Prioridad:** 1 Crítico.

**Ampliar información:**

<https://www.bleepingcomputer.com/news/security/critical-ivanti-rce-flaw-with-public-exploit-now-used-in-attacks/>

---

**Vulnerabilidad en más de 700,000 routers DrayTek expone a ataques remotos**

Investigadores de seguridad han descubierto varias vulnerabilidades críticas en routers DrayTek que afectan a más de 700,000 dispositivos en todo el mundo. Estas fallas permiten a actores malintencionados ejecutar ataques de ejecución remota de código (RCE), comprometiendo potencialmente toda la red de los usuarios afectados. Aunque aún no se han asignado CVEs específicos para estas vulnerabilidades, la preocupación es alta debido a la escala de dispositivos expuestos, además de su uso en hogares y pequeñas empresas.

Para mitigar este riesgo, se recomienda actualizar de inmediato el firmware de los dispositivos DrayTek a las últimas versiones disponibles, que han sido publicadas por el fabricante para corregir estas fallas. Además, se sugiere deshabilitar la gestión remota si no es necesaria, utilizar contraseñas fuertes y activar el firewall en los routers afectados.

**Prioridad:** 3 Importante.

**Ampliar información:**

<https://thehackernews.com/2024/10/alert-over-700000-draytek-routers.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

### **Falsas actualizaciones de navegadores distribuyen WarmCookie, una nueva versión de malware**

Un actor conocido como 'SocGolish' está propagando una variante del malware WarmCookie mediante campañas de falsas actualizaciones de navegadores. El malware se distribuye a través de sitios web comprometidos que muestran notificaciones falsas de actualización para aplicaciones como Google Chrome, Firefox, y Java. Este esquema fue identificado por los investigadores de Gen Threat Labs.

El malware WarmCookie es un backdoor que permite la ejecución remota de comandos, robo de datos y captura de pantallas. Se recomienda evitar descargar actualizaciones de fuentes no oficiales y siempre verificar que provengan directamente de los sitios web oficiales de los navegadores.

**Prioridad:** 2 Urgente.

**Ampliar información:**

<https://www.bleepingcomputer.com/news/security/fake-browser-updates-spread-updated-warmcookie-malware/>

---

**Malware disfrazado de solicitudes de empleo afecta a reclutadores**

Un actor de amenazas conocido como Golden Chickens está distribuyendo el malware "More\_eggs" mediante campañas de spear-phishing dirigidas a reclutadores. El ataque se propaga a través de correos electrónicos que simulan solicitudes de empleo, incluyendo archivos maliciosos disfrazados de currículos. Trend Micro identificó este malware, que permite robar credenciales bancarias, correos y datos administrativos. More\_eggs, un malware-as-a-service (MaaS), realiza un reconocimiento del sistema, estableciendo una conexión con un servidor C2 para recibir payloads adicionales.

Para mitigar estos ataques, se recomienda entrenar al personal en la detección de phishing, usar herramientas de análisis de archivos y aplicar políticas de ejecución de scripts solo para aplicaciones confiables.

**Prioridad:** 3 Importante.

**Ampliar información:**

<https://thehackernews.com/2024/10/fake-job-applications-deliver-dangerous.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

### Colaboración global contra LockBit y Evil Corp culmina en arrestos

Una operación internacional, denominada "Operación Cronos", liderada por Europol, ha resultado en la detención de cuatro individuos y la desactivación de nueve servidores relacionados con el ransomware LockBit. Entre los arrestados está un desarrollador del grupo en Francia, así otros asociados en Reino Unido y España. Además, Aleksandr Ryzhenkov, vinculado a Evil Corp, ha sido sancionado por su papel en la distribución del malware Dridex. Identificado por Europol y el Departamento de Justicia de EE. UU., las autoridades recomiendan robustecer las defensas contra el ransomware..

**Prioridad:** 3 Importante.

**Ampliar información:**

<https://thehackernews.com/2024/10/lockbit-ransomware-and-evil-corp.html>

---

## **Cloudflare bloquea el ataque DDoS más grande registrado, alcanzando 3.8 Tbps**

Cloudflare ha bloqueado un ataque de denegación de servicio distribuido (DDoS) que alcanzó un pico de 3.8 Tbps, el más grande registrado hasta la fecha. El ataque dirigido a sectores financieros, de telecomunicaciones e Internet fue parte de una campaña de ataques volumétricos que inundaron la infraestructura de red con datos basura. La red de dispositivos comprometidos incluía routers Asus y MikroTik, DVRs y servidores web. El ataque duró 65 segundos, y Cloudflare lo mitigó de manera automática.

**Prioridad:** 3 Importante.

### **Ampliar información:**

<https://www.bleepingcomputer.com/news/security/cloudflare-blocks-largest-recorded-ddos-attack-peaking-at-38tbps/>

---

