Investigadores en ciberseguridad han revelado tres vulnerabilidades en Rack, la interfaz del servidor web para Ruby. De ser explotadas con éxito, podrían permitir a atacantes acceder sin autorización a archivos, inyectar datos maliciosos y alterar registros en ciertas condiciones.

La empresa de ciberseguridad OPSWAT identificó estas fallas, que son:

- CVE-2025-27610 (puntuación CVSS: 7.5): Vulnerabilidad de *path traversal* que permite acceder a cualquier archivo dentro del directorio raíz especificado, siempre que el atacante conozca la ruta.
- CVE-2025-27111 (puntuación CVSS: 6.9): Vulnerabilidad de neutralización inadecuada de saltos de línea (CRLF) y de salida en los registros, que podría ser usada para manipular y distorsionar los archivos de log.
- CVE-2025-25184 (puntuación CVSS: 5.7): Similar a la anterior, esta falla también permite alterar los registros e inyectar datos maliciosos.

Si estas vulnerabilidades son explotadas, un atacante podría ocultar rastros de sus acciones, leer archivos arbitrarios e insertar código dañino.

Entre ellas, la más grave es CVE-2025-27610, ya que permitiría a atacantes no autenticados acceder a información sensible como configuraciones, credenciales y datos confidenciales, aumentando el riesgo de filtraciones, según el reporte de OPSWAT.

El problema radica en que el middleware Rack::Static, utilizado para servir archivos estáticos (como JavaScript, hojas de estilo o imágenes), no filtra adecuadamente las rutas proporcionadas por los usuarios. Esto puede permitir que un atacante construya rutas maliciosas para acceder a archivos fuera del directorio previsto.

En concreto, si el parámetro :root no se define explícitamente, Rack lo establece automáticamente como el directorio de trabajo actual (*Dir.pwd*), tratándolo como raíz del sitio web. Así, si :root no está definido o está mal configurado respecto al parámetro :urls, un atacante podría usar técnicas de *path traversal* para acceder a archivos sensibles fuera del

área pública.

Medidas de mitigación:
Se recomienda actualizar a la última versión de Rack. Si no es posible aplicar el parche de inmediato, se sugiere eliminar el uso de Rack::Static o asegurarse de que el parámetro root: apunte solo a un directorio con archivos públicos.

## Vulnerabilidad crítica en Infodraw Media Relay Service

Además, se ha descubierto una grave falla de seguridad en el servicio Infodraw Media Relay Service (MRS), relacionada con *path traversal* en el parámetro de nombre de usuario durante el inicio de sesión (CVE-2025-43928, puntuación CVSS: 9.8).

Infodraw, una empresa israelí de soluciones de videovigilancia móvil, fabrica dispositivos que transmiten datos de audio, video y GPS a través de redes de telecomunicaciones. Sus productos son utilizados por fuerzas policiales, investigadores privados, gestión de flotas y transporte público en varios países.

El investigador Tim Philipp Schäfers explicó que la vulnerabilidad permite a atacantes no autenticados leer cualquier archivo del sistema de manera trivial. Además, existe una vulnerabilidad adicional que permite borrar archivos arbitrarios del sistema.

La falla afecta tanto a versiones de Windows como de Linux del MRS. Aunque algunos sistemas vulnerables en Bélgica y Luxemburgo fueron desconectados tras las advertencias, no existe un parche disponible por parte del fabricante.

Recomendaciones:
Las organizaciones afectadas deberían desconectar inmediatamente las aplicaciones vulnerables. Si esto no es posible, se recomienda proteger los sistemas mediante una VPN o restringiendo el acceso por direcciones IP específicas, ya que es probable que atacantes intenten explotar esta vulnerabilidad pronto.