

Reporte: Para la versión de Apache 2.4.62 no se encontraron vulnerabilidades específicas, dejo y expongo vulnerabilidades que soluciona dicha versión.

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
80	HTTP	APACHE 2.4.62	CVE-2024-40898	La SSRF en el servidor HTTP Apache en Windows con mod_rewrite en el contexto servidor/vhost permite filtrar hashes NTML a un servidor malicioso mediante SSRF y solicitudes maliciosas. Se recomienda a los usuarios actualizar a la versión 2.4.62, que soluciona este problema.	https://nvd.nist.gov/vuln/detail/CVE-2024-40898
80	HTTP	APACHE 2.4.62	CVE-2024-40725	Una corrección parcial para CVE-2024-39884 en el núcleo de Apache HTTP Server 2.4.61 ignora el uso de la configuración heredada de los controladores basada en el tipo de contenido. "AddType" y configuraciones similares, en ciertas circunstancias donde se solicitan archivos indirectamente, resultan en la divulgación del código fuente de contenido local. Por ejemplo, los scripts PHP pueden ser servidos en lugar de interpretados. Se recomienda a los usuarios actualizar a la versión 2.4.62, que soluciona este problema.	https://nvd.nist.gov/vuln/detail/CVE-2024-40725