Search Parameters:

- Results Type: Overview
- Keyword (text search): apache 2.4.62
- Search Type: Search All
- CPE Name Search: false

There are **2** matching records.

Displaying matches **1** through **2**.

Vuln ID	Summary	CVSS Severity
CVE-2024-40898	SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue. **Published:** July 18, 2024; 6:15:03 AM -0400	*V4.0:*(not available) *V3.1:* 7.5 HIGH *V2.0:*(not available)
CVE-2024-40725	A partial fix for CVE-2024-39884 in the core of Apache HTTP Server 2.4.61 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP scripts may be served instead of interpreted. Users are recommended to upgrade to version 2.4.62, which fixes this issue. **Published:** July 18, 2024; 6:15:02 AM -0400	*V4.0:*(not available) *V3.1:* 5.3 MEDIUM *V2.0:*(not available)