TLP: CLEAR : Se usa cuando la información no genera ningún riesgo de mal uso y pueda ser difundido de forma pública. En este sentido, la información puede ser distribuida sin restricciones, pero sujeta a controles de derechos de autor

Julio 18 de 2024

INFORME DE VULNERABILDIAD EN SERVICIO APACHE CVE-2024-40725 CVE-2024-40898

Se informa de una corrección parcial relacionada con el **CVE-2024-39884** en el núcleo de Apache HTTP Server 2.4.61, que ignora el uso de la configuración heredada basada en el tipo de contenido de los controladores. "AddType", lo cual da como resultado la divulgación del código fuente del contenido.[1]

Ejemplo, los scripts PHP pueden ser servidos en lugar de interpretados.

Detalles de la Vulnerabilidad:

- CVE-2024-40725[2]
- CVE-2024-40898[3]
- Impacto: Divulgación del código fuente del contenido
- Versiones afectadas: **2.4.60** hasta la **2.4.61**

Recomendaciones de remediación:

- Actualizar Apache a versión **2.4.62**

Cordialmente

CSIRT Académico UNAD
Correo electrónico: csirt@unad.edu.co
(+57 1) 344 37 00 Ext. 1042516

[1] Récord CVE | CVE
[2] CVE - CVE-2024-40725 (mitre.org)
[3] CVE - CVE-2024-40898 (mitre.org)