DB Update CVE-2024-25117 - Score: 6.8

dompdf php-svg-lib *
php php *

Description:

php-svg-lib is a scalable vector graphics (SVG) file parsing/
rendering library. Prior to version 0.5.2, php-svg-lib fails to
validate that font-family doesn't contain a PHAR url, which
might leads to RCE on PHP < 8.0, and doesn't validate if
external references are allowed. This might leads to bypass of
restrictions or RCE on projects that are using it, if they do
not strictly revalidate the fontName that is passed by php-svglib. The 'Style::fromAttributes('), or the 'Style::parseCssStyle
()' should check the content of the 'font-family' and prevents
it to use a PHAR url, to avoid passing an invalid and dangerous
'fontName' value to other libraries. The same check as done in
the 'Style::fromStyleSheets' might be reused. Libraries using
this library as a dependency might be vulnerable to some bypass
of restrictions, or even remote code execution, if they do not
double check the value of the 'fontName' that is passed by phpsvg-lib. Version 0.5.2 contains a fix for this issue.

Main problems:

502 "Descrialization of Untrusted Data"