NVD DB Update

CVE-2025-0366 - Score: 8.8

Components:

artbees jupiter x core *

Description:

The Jupiter X Core plugin for WordPress is vulnerable to Local File Inclusion to Remote Code Execution in all versions up to, and including, 4.8.7 via the get_svg() function. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution. In this specific case, an attacker can create a form that allows SVG uploads, upload an SVG file with malicious content and then include the SVG file in a post to achieve remote code execution. This means it is relatively easy to gain remote code execution as a contributor-level user and above by default.

Main problems:

98 no CWE Description available