NVD DB Update

CVE-2023-25828 - Score: 7.2

Components:

pluck-cms pluck *
pluck-cms pluck 4.7.16

Description:

Pluck CMS is vulnerable to an authenticated remote code execution (RCE) vulnerability through its albums module. Albums are used to create collections of images that can be inserted into web pages across the site. Albums allow the upload of various filetypes, which undergo a normalization process before being available on the site. Due to lack of file extension validation, it is possible to upload a crafted JPEG payload containing an embedded PHP web-shell. An attacker may navigate to it directly to achieve RCE on the underlying web server. Administrator credentials for the Pluck CMS web interface are required to access the albums module feature, and are thus required to exploit this vulnerability. CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H /I:H/A:H/E:P/RL:O/RC:C (8.2 High)

Main problems:

434 "Unrestricted Upload of File with Dangerous Type"