CVE

Upload Malicious File in mojoPortal v2.7 (CVE-2022-40341)

Vulnerability Type: Upload Malicious File

Vendor of Product: mojoPortal

Discoverer: Dat Hoang and Duy Anh of VietSunshine Cyber Security Services

Affected version: mojoPortal - 2.7

Attack Type: Remote

Description: mojoPortal v2.7 was discovered to contain an arbitrary file upload vulnerability which allows attackers to execute arbitrary code via a crafted PNG file.

Impact: Remote code execution

Attack vector

An attacker requires an account. An attacker does the following steps:

> - **Step 1:** An authenticated attacker could access URL: https://{IP]/Admin/FileManagerAlt.aspx to use the File Manager feature.
> - **Step 2:** Upload a png file containing malicious aspx code
> - **Step 3:** Rename the uploaded file extension from png to aspx
> - **Step 4:** Access URL https://{IP]/Data/Sites/1/media/[filename] to get the webshell

Previous
Directory Traversal in mojoPortal v2.7 (CVE-2022-40123)

Last modified 1mo ago