C

CVE-2020-9471

Project ID: 17453022

Umbraco Cloud 8.5.3 allows an authenticated file upload (and consequently Remote Code Execution) via the Install Packages function...

Update README.md
eLeN3Re authored 2 years ago

Name	Last commit	Last update
img	Upload New File	2 years ago
README.md	Update README.md	2 years ago
exploit_cloud.py	Upload	2 years ago

README.md

Umbraco Cloud 8.5.3 - Authenticated FileUpload PoC

Attack Type: File Upload

Product Version: 8.5.3

OWASP Category: Unrestricted File Upload

Solution: Add package integrity mechanisms and/or file extension whitelist/blacklist filtering

Summary: Umbraco Cloud 8.5.3 allows an authenticated file upload via the Packages functionality

Technical Description: See https://gitlab.com/eLeN3Re/cve-2020-9472/-/blob/master/CVE-2020-9472.pdf. The impact in this case is different since anyone can register a bogus account in the Umbraco Cloud (which will not be email verified) and then exploit the file upload for achieving RCE in the Umbraco cloud infrastructure.

Exploit: See exploit_cloud.py