

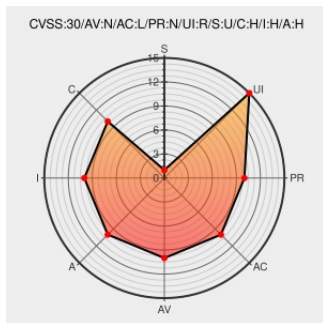


# CVE-2018-5969

Published on: 01/24/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:45 PM UTC

## CVE-2018-5969

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Photography Cms](#) from [Photography Cms Project](#) contain the following vulnerability:

Cross Site Request Forgery (CSRF) exists in Photography CMS 1.0 via clients/resources/ajax/ajax\_new\_admin.php, as demonstrated by adding an admin account.

CVE-2018-5969 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.8 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description                                                                        | Tags                                                                                                                                                                     | Link                             |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| Photography CMS 1.0 - Cross-Site Request Forgery (Add Admin) - PHP webapps Exploit | <a href="#">Third Party Advisory</a><br><a href="#">VDB Entry</a><br><a href="#">www.exploit-db.com</a><br><a href="#">Proof of Concept</a><br><a href="#">text/html</a> | <a href="#">EXPLOIT-DB 43867</a> |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type                                                             | Vendor                                  | Product                         | Version | Update | Edition | Language |
|------------------------------------------------------------------|-----------------------------------------|---------------------------------|---------|--------|---------|----------|
| Application                                                      | <a href="#">Photography Cms Project</a> | <a href="#">Photography Cms</a> | 1.0     | All    | All     | All      |
| Application                                                      | <a href="#">Photography Cms Project</a> | <a href="#">Photography Cms</a> | 1.0     | All    | All     | All      |
| cpe:2.3:a:photography_cms_project:photography_cms:1.0:*:*:*:*:*: |                                         |                                 |         |        |         |          |
| cpe:2.3:a:photography_cms_project:photography_cms:1.0:*:*:*:*:*: |                                         |                                 |         |        |         |          |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)