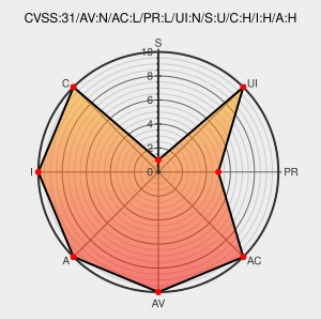
# CVE-2021-24892

Published on: 11/23/2021 12:00:00 AM UTC

Last Modified on: 11/29/2021 03:44:00 PM UTC

## CVE-2021-24892

Source: Mitre | Source: Nist | Print: PDF




Certain versions of Advanced Forms from Advanced Forms Project contain the following vulnerability:

Insecure Direct Object Reference in edit function of Advanced Forms (Free & Pro) before 1.6.9 allows authenticated remote attacker to change arbitrary user's email address and request for reset password, which could lead to take over of WordPress's administrator account. To exploit this vulnerability, an attacker must register to obtain a valid WordPress's user and use such user to authenticate with WordPress in order to exploit the vulnerable edit function.

CVE-2021-24892 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **TODO** - **Advanced Forms Ppro** version **< 1.6.9**

Affected Vendor/Software: **TODO** - **Advanced Forms** version **< 1.6.9**

CVSS3 Score: 8.8 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | LOW | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

CVSS2 Score: 6.5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | SINGLE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

## CVE References

| Description | Tags | Link |
|---|---|---|
| Attention Required! \| Cloudflare | wpscan.com text/html Inactive Link Not Archived | MISC wpscan.com/vulnerability/364b0843-a990-4204-848a-60c928cc5bc0 |
| Added form nonce with arguments · advancedforms/advanced-forms@2ce3ab6 · GitHub | github.com text/html | MISC github.com/advancedforms/advanced-forms/commit/2ce3ab6985c3a909eefb01c562995bc6a994d3a2 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Advanced Forms Project | Advanced Forms | All | All | All | All |
| Application | Advanced Forms Project | Advanced Forms | All | All | All | All |

cpe:2.3:a:advanced_forms_project:advanced_forms:*:*:*:*:free:wordpress:*:*:

cpe:2.3:a:advanced_forms_project:advanced_forms:*:*:*:*:pro:wordpress:*:*:

## Discovery Credit

Suppawit Punhakit

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @CVEreport | CVE-2021-24892 : Insecure Direct Object Reference in edit function of Advanced Forms Free & Pro before 1.6.9 allo… twitter.com/i/web/status/1… | 2021-11-23 19:50:37 |
| @LinInfoSec | Wordpress - CVE-2021-24892: wpscan.com/vulnerability/… | 2021-11-23 21:36:12 |

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status** status.cve.report