3

Incorrect Authorization Checks in /include/findusers.php

Share:

TIMELINE

egix submitted a report to ImpressCMS. Jan 18th (2 years ago)

Summary:

The vulnerability is located in the `/include/findusers.php` script:

Code 390 Bytes Wrap lines Copy Download

```
16.   include "../mainfile.php";
17.   xoops_header(false);
18.
19.   $denied = true;
20.   if (!empty($_REQUEST['token'])) {
21.       if (icms::$security->validateToken($_REQUEST['token'], false)) {
22.           $denied = false;
23.       }
24.   } elseif (is_object(icms::$user) && icms::$user->isAdmin()) {
25.       $denied = false;
26.  }
27.  if ($denied) {
28.      icms_core_Message::error(_NOPERM);
29.      exit();
30.  }
```

As far as I can see, I believe this script should be accessible by admin users only (due to line 24). However, because of the if statements at lines 20-23, this script could be accessed by unauthenticated attackers if they will provide a valid security token. Such a token will be generated in several places within the application (just search for the string `icms::$security->getTokenHTML()`), and some of them do not require the user to be authenticated, like in `misc.php` at line 181.

ImpressCMS branch :

The vulnerability has been tested and confirmed on ImpressCMS version 1.4.2 (the latest at the time of writing).

Steps To Reproduce:

1. Try to access the `/include/findusers.php` script without being logged into the application
2. You will see an error message saying **"Sorry, you don't have permission to access this area."**
3. Go to `/misc.php?action=showpopups&type=friend` and look at the HTML source code, search the string `XOOPS_TOKEN_REQUEST` and copy the value of the token
4. Go to `/include/findusers.php?token=[TOKEN_VALUE]` and you will be able to access the script and e.g. search through the registered users

Impact

This vulnerability might allow unauthenticated attackers to access an otherwise restricted functionality of the application, which in turn might allow an information disclosure about the CMS users (specifically, only the username and real name will be disclosed).

fiammybe ImpressCMS staff changed the status to **Triaged**. Jan 29th (2 years ago)

egix posted a comment. Feb 3rd (2 years ago)

Hi @fiammybe,

the Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2021-26598 to this vulnerability.

egix posted a comment. Dec 30th (12 months ago)

Hi,

Just wanted to let you know I've retested this issue with version **1.4.3-rc** and it's still exploitable!

skenow ImpressCMS staff posted a comment. Dec 30th (12 months ago)

Thank you for testing and letting us know. The RC does not include the work being done on this issue and there will be an RC 2 release coming

egix posted a comment. Updated Feb 11th (10 months ago)

Hi @fiammybe @skenow,

I THINK this issue is not yet completely fixed. So, basically this is the new code:

Code 308 Bytes Wrap lines Copy Download

```
$denied = true;

if (!empty($_REQUEST['token']) && is_object(icms::$user)) {
 if (icms::$security->validateToken($_REQUEST['token'], false)) {
     $denied = false;
 }
} elseif (is_object(icms::$user) && icms::$user->isAdmin()) {
 $denied = false;
}
```

```
}
```

What if a non-admin user access this page providing a token retrieved in another page? I believe they will be able to access the findusers script, even though they are not admin users - because the first `if` statement will be triggered and the token is valid, so `$denied` is being set to **false**.

I said "I THINK" because at the moment I can't test this on my local ImpressCMS installation: when I try to add new users I get an error message which says "Could not register new user."...

skenow ImpressCMS staff posted a comment. Feb 15th (10 months ago)

This report seems to be specific to the session authentication, which has been addressed. The SQLi issue (#1081145) is yet to be resolved.

Could we close this one?

fiammybe ImpressCMS staff closed the report and changed the status to Resolved. Feb 16th (10 months ago)

This was resolved in ImpressCMS 1.4.3

egix posted a comment. Feb 16th (10 months ago)

Hi @skenow @fiammybe

This report is about an **Incorrect Authorization** vulnerability, and not about "session authentication". Before your fix this issue could have been exploited by both authenticated and unauthenticated attackers; now it can only be exploited by authenticated users. But the issue still exists: non-admin users can access a feature which is intended for admin users only. I know the impact is quite low (information disclosure about the CMS users), but the vulnerability is still present in ImpressCMS 1.4.3.

skenow ImpressCMS staff posted a comment. Feb 19th (10 months ago)

@egix - this is not an admin-only feature. It is also used in the front-end for user searches by authenticated users.

egix posted a comment. Feb 20th (10 months ago)

Ok, sorry... I misunderstood then. In this case I would say this report is about an authentication bypass vulnerability, which is now resolved in ImpressCMS 1.4.3.

egix requested to disclose this report. Feb 20th (10 months ago)

This report has been disclosed. Mar 22nd (9 months ago)