[KIS-2022-03] ImpressCMS <= 1.4.2 (findusers.php) Incorrect Access Control Vulnerability

From: Egidio Romano <research () karmainsecurity com>
Date: Tue, 22 Mar 2022 13:02:46 +0100

```
------------------------------------------------------------------------
ImpressCMS <= 1.4.2 (findusers.php) Incorrect Access Control Vulnerability
------------------------------------------------------------------------


[-] Software Link:

https://www.impresscms.org


[-] Affected Versions:

Version 1.4.2 and prior versions.


[-] Vulnerability Description:

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

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.    }        }

This script should be accessible to authenticated users only. However, because of the "if" statement 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, and some of them do not require the user to be
authenticated, like in the misc.php script. This might be exploited to access an otherwise restricted functionality of
the application, which in turn might allow an information disclosure about the CMS users.


[-] Solution:

Upgrade to version 1.4.3 or later.


[-] Disclosure Timeline:

[19/01/2021] - Vendor notified through HackerOne
[03/02/2021] - CVE number assigned
[06/02/2022] - Version 1.4.3 released
[22/03/2022] - Public disclosure


[-] CVE Reference:

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


[-] Credits:

Vulnerability discovered by Egidio Romano.


[-] Other References:

https://hackerone.com/reports/1081137


[-] Original Advisory:

http://karmainsecurity.com/KIS-2022-03
```