[KIS-2022-02] ImpressCMS <= 1.4.2 (image-edit.php) Path Traversal Vulnerability

From: Egidio Romano <research () karmainsecurity com>
Date: Tue, 22 Mar 2022 13:01:53 +0100

```
-----------------------------------------------------------------
ImpressCMS <= 1.4.2 (image-edit.php) Path Traversal Vulnerability
-----------------------------------------------------------------
```

[-] Software Link:

https://www.impresscms.org

[-] Affected Versions:

Version 1.4.2 and prior versions.

[-] Vulnerability Description:

The vulnerability is located in the /libraries/image-editor/image-edit.php script:

```
161.        if (@copy ( ICMS_IMANAGER_FOLDER_PATH . '/temp/' . $simage_temp, $categ_path . $simage->getVar (
'image_name' ) )) { 162.            if (@unlink ( ICMS_IMANAGER_FOLDER_PATH . '/temp/' . $simage_temp )) {
163.                $msg = _MD_AM_DBUPDATED;

[...]

190.        } else {
191.            if (copy ( ICMS_IMANAGER_FOLDER_PATH . '/temp/' . $simage_temp, $categ_path . $imgname )) { 192.
            @unlink ( ICMS_IMANAGER_FOLDER_PATH . '/temp/' . $simage_temp );
193.            }
```

User input passed through the "image_temp" parameter is not properly sanitized before being used in a call to the unlink() function at lines 162 and 192. This can be exploited by authenticated attackers to carry out Path Traversal attacks and delete arbitrary files in the context of the web server process. This vulnerability could be exploited also to disclose the content of arbitrary files in case the web server allows for directory listing.

[-] Solution:

Upgrade to version 1.4.3 or later.

[-] Disclosure Timeline:

[19/01/2021] - Vendor notified through HackerOne
[29/01/2021] - Vulnerability acknowledged by the vendor
[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-2021-26601 to this vulnerability.

[-] Credits:

Vulnerability discovered by Egidio Romano.

[-] Other References:

https://hackerone.com/reports/1081878

[-] Original Advisory:

http://karmainsecurity.com/KIS-2022-02

____
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/

Current thread:

- **[KIS-2022-02] ImpressCMS <= 1.4.2 (image-edit.php) Path Traversal Vulnerability** *Egidio Romano (Mar 22)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License