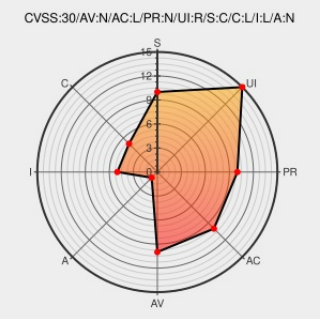
# CVE-2018-17314

Published on: 09/26/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:20 PM UTC

## CVE-2018-17314

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Mp 305 from Ricoh contain the following vulnerability:

On the RICOH Aficio MP 305+ printer, HTML Injection and Stored XSS vulnerabilities have been discovered in the area of adding addresses via the entryNameIn parameter to /web/entry/en/address/adrsSetUserWizard.cgi.

CVE-2018-17314 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 6.1 - MEDIUM

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

### CVSS2 Score: 4.3 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | PARTIAL | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| RICOH MP 305+ Printer Cross Site Scripting ≈ Packet Storm | Exploit<br>Third Party Advisory<br>VDB Entry<br>packetstormsecurity.com<br>text/html | MISC packetstormsecurity.com/files/149501/RICOH-MP-305-Printer-Cross-Site-Scripting.html |

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.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Hardware | Ricoh | Mp 305 | - | All | All | All |
| Operating System | Ricoh | Mp 305 Firmware | - | All | All | All |
| Hardware | Ricoh | Mp 305 | - | All | All | All |
| Hardware | Ricoh | Mp 305 | - | All | All | All |
| Operating System | Ricoh | Mp 305 Firmware | - | All | All | All |
| Operating System | Ricoh | Mp 305 Firmware | - | All | All | All |

cpe:2.3:h:ricoh:mp_305+:-:*:*:*:*:*:*:*:

cpe:2.3:o:ricoh:mp_305+_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:ricoh:mp_305\+:-:*:*:*:*:*:*:*:

cpe:2.3:h:ricoh:mp_305\+:-:*:*:*:*:*:*:*:

cpe:2.3:o:ricoh:mp_305\+_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:ricoh:mp_305\+_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→