



# CVE-2015-2344

Published on: 03/16/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:20 PM UTC

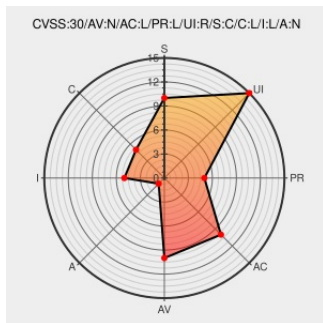
## CVE-2015-2344

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in VMware vRealize Automation 6.x before 6.2.4 on Linux allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.

CVE-2015-2344 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.4 - MEDIUM**

| Attack Vector  | Attack Complexity      | Privileges Required | User Interaction    |
|----------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b> | <b>LOW</b>             | <b>LOW</b>          | <b>REQUIRED</b>     |
| Scope          | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>CHANGED</b> | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |

CVSS2 Score: **3.5 - LOW**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>SINGLE</b>       |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>PARTIAL</b>    | <b>NONE</b>         |

## CVE References

| Description                                                                                              | Tags                                                                 | Link                                                                                |
|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| VMware vRealize Input Validation Flaws Let Remote Conduct Cross-Site Scripting Attacks - SecurityTracker | <a href="#">www.securitytracker.com</a><br><a href="#">text/html</a> | <a href="#">SECTrack 1035270</a>                                                    |
| VMSA-2016-0003   United States                                                                           | <a href="#">Vendor Advisory</a><br><a href="#">www.vmware.com</a>    | <a href="#">CONFIRM</a><br><a href="#">www.vmware.com/security/advisories/VMSA-</a> |

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type                                                      | Vendor | Product             | Version | Update | Edition | Language |
|-----------------------------------------------------------|--------|---------------------|---------|--------|---------|----------|
| Operating System                                          | Linux  | Linux Kernel        | All     | All    | All     | All      |
| Operating System                                          | Linux  | Linux Kernel        | All     | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.0     | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.0.1   | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.0.1.1 | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.0.1.2 | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.1     | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.1.1   | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.2     | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.2.1   | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.2.2   | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.2.3   | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.0     | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.0.1   | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.0.1.1 | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.0.1.2 | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.1     | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.1.1   | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.2     | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.2.1   | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.2.2   | All    | All     | All      |
| Application                                               | Vmware | Vrealize Automation | 6.2.3   | All    | All     | All      |
| cpe:2.3:o:linux:linux_kernel:*.*.*.*.*.*.*.*:             |        |                     |         |        |         |          |
| cpe:2.3:o:linux:linux_kernel:*.*.*.*.*.*.*.*:             |        |                     |         |        |         |          |
| cpe:2.3:a:vmware:vrealize_automation:6.0:*.*.*.*.*.*.*.*: |        |                     |         |        |         |          |

|                                                         |
|---------------------------------------------------------|
| cpe:2.3:a:vmware:vrealize_automation:6.0.1:*:*:*:*:*:   |
| cpe:2.3:a:vmware:vrealize_automation:6.0.1.1:*:*:*:*:*: |
| cpe:2.3:a:vmware:vrealize_automation:6.0.1.2:*:*:*:*:*: |
| cpe:2.3:a:vmware:vrealize_automation:6.1:*:*:*:*:*:     |
| cpe:2.3:a:vmware:vrealize_automation:6.1.1:*:*:*:*:*:   |
| cpe:2.3:a:vmware:vrealize_automation:6.2:*:*:*:*:*:     |
| cpe:2.3:a:vmware:vrealize_automation:6.2.1:*:*:*:*:*:   |
| cpe:2.3:a:vmware:vrealize_automation:6.2.2:*:*:*:*:*:   |
| cpe:2.3:a:vmware:vrealize_automation:6.2.3:*:*:*:*:*:   |
| cpe:2.3:a:vmware:vrealize_automation:6.0:*:*:*:*:*:     |
| cpe:2.3:a:vmware:vrealize_automation:6.0.1:*:*:*:*:*:   |
| cpe:2.3:a:vmware:vrealize_automation:6.0.1.1:*:*:*:*:*: |
| cpe:2.3:a:vmware:vrealize_automation:6.0.1.2:*:*:*:*:*: |
| cpe:2.3:a:vmware:vrealize_automation:6.1:*:*:*:*:*:     |
| cpe:2.3:a:vmware:vrealize_automation:6.1.1:*:*:*:*:*:   |
| cpe:2.3:a:vmware:vrealize_automation:6.2:*:*:*:*:*:     |
| cpe:2.3:a:vmware:vrealize_automation:6.2.1:*:*:*:*:*:   |
| cpe:2.3:a:vmware:vrealize_automation:6.2.2:*:*:*:*:*:   |
| cpe:2.3:a:vmware:vrealize_automation:6.2.3:*:*:*:*:*:   |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)