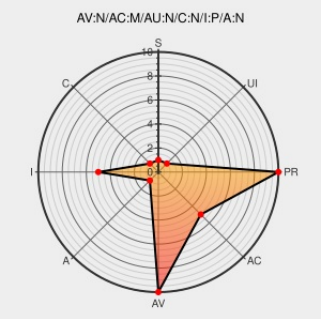
# CVE-2015-6939

Published on: 09/18/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

## CVE-2015-6939

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




Certain versions of Joomla! from Joomla contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the login module in Joomla! 3.4.x before 3.4.4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

CVE-2015-6939 has been assigned by cve@mitre.org to track the vulnerability

### 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 |
|---|---|---|
| Joomla! Input Validation Flaw in Login Module Lets Remote Conduct Cross-Site Scripting Attacks - SecurityTracker | Third Party Advisory, VDB Entry, www.securitytracker.com, text/html | SECTRACK 1033541 |
| [20150908] - Core - XSS Vulnerability | Vendor Advisory, developer.joomla.org, text/html | CONFIRM developer.joomla.org/security-centre/626-20150908-core-xss-vulnerability.html |
| Joomla! CMS 3.4.3 Cross Site Scripting ≈ Packet Storm | Exploit, Third Party Advisory, packetstormsecurity.com, text/html | MISC packetstormsecurity.com/files/133907/Joomla-CMS-3.4.3-Cross-Site-Scripting.html |

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 |
|---|---|---|---|---|---|---|
| Application | Joomla | Joomla! | 3.4.0 | All | All | All |
| Application | Joomla | Joomla! | 3.4.0 | alpha | All | All |
| Application | Joomla | Joomla! | 3.4.0 | beta1 | All | All |
| Application | Joomla | Joomla! | 3.4.0 | beta2 | All | All |
| Application | Joomla | Joomla! | 3.4.0 | beta3 | All | All |
| Application | Joomla | Joomla! | 3.4.0 | rc1 | All | All |
| Application | Joomla | Joomla! | 3.4.1 | All | All | All |
| Application | Joomla | Joomla! | 3.4.1 | rc1 | All | All |
| Application | Joomla | Joomla! | 3.4.1 | rc2 | All | All |
| Application | Joomla | Joomla! | 3.4.2 | All | All | All |
| Application | Joomla | Joomla! | 3.4.2 | rc1 | All | All |
| Application | Joomla | Joomla! | 3.4.3 | All | All | All |
| Application | Joomla | Joomla! | 3.4.0 | All | All | All |
| Application | Joomla | Joomla! | 3.4.0 | alpha | All | All |
| Application | Joomla | Joomla! | 3.4.0 | beta1 | All | All |
| Application | Joomla | Joomla! | 3.4.0 | beta2 | All | All |
| Application | Joomla | Joomla! | 3.4.0 | beta3 | All | All |
| Application | Joomla | Joomla! | 3.4.0 | rc1 | All | All |
| Application | Joomla | Joomla! | 3.4.1 | All | All | All |
| Application | Joomla | Joomla! | 3.4.1 | rc1 | All | All |
| Application | Joomla | Joomla! | 3.4.1 | rc2 | All | All |
| Application | Joomla | Joomla! | 3.4.2 | All | All | All |
| Application | Joomla | Joomla! | 3.4.2 | rc1 | All | All |
| Application | Joomla | Joomla! | 3.4.3 | All | All | All |
| Application | Joomla | Joomla! | 3.4.0 | All | All | All |
| Application | Joomla | Joomla! | 3.4.0 | alpha | All | All |
| Application | Joomla | Joomla! | 3.4.0 | beta1 | All | All |
| Application | Joomla | Joomla! | 3.4.0 | beta2 | All | All |
| Application | Joomla | Joomla! | 3.4.0 | beta3 | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Joomla | Joomla! | 3.4.0 | rc1 | All | All |
| Application | Joomla | Joomla! | 3.4.1 | All | All | All |
| Application | Joomla | Joomla! | 3.4.1 | rc1 | All | All |
| Application | Joomla | Joomla! | 3.4.1 | rc2 | All | All |
| Application | Joomla | Joomla! | 3.4.2 | All | All | All |
| Application | Joomla | Joomla! | 3.4.2 | rc1 | All | All |
| Application | Joomla | Joomla! | 3.4.3 | All | All | All |

cpe:2.3:a:joomla:joomla!:3.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla!:3.4.0:alpha:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla!:3.4.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla!:3.4.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla!:3.4.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla!:3.4.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla!:3.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla!:3.4.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla!:3.4.1:rc2:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla!:3.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla!:3.4.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla!:3.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla\!:3.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla\!:3.4.0:alpha:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla\!:3.4.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla\!:3.4.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla\!:3.4.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla\!:3.4.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla\!:3.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla\!:3.4.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla\!:3.4.1:rc2:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla\!:3.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:joomla:joomla\!:3.4.2:rc1:*:*:*:*:*:*:

| |
|---|
| cpe:2.3:a:joomla:joomla\!:3.4.3:*:*:*:*:*:*:* |
| cpe:2.3:a:joomla:joomla\!:3.4.0:*:*:*:*:*:*:* |
| cpe:2.3:a:joomla:joomla\!:3.4.0:alpha:*:*:*:*:*:* |
| cpe:2.3:a:joomla:joomla\!:3.4.0:beta1:*:*:*:*:*:* |
| cpe:2.3:a:joomla:joomla\!:3.4.0:beta2:*:*:*:*:*:* |
| cpe:2.3:a:joomla:joomla\!:3.4.0:beta3:*:*:*:*:*:* |
| cpe:2.3:a:joomla:joomla\!:3.4.0:rc1:*:*:*:*:*:* |
| cpe:2.3:a:joomla:joomla\!:3.4.1:*:*:*:*:*:*:* |
| cpe:2.3:a:joomla:joomla\!:3.4.1:rc1:*:*:*:*:*:* |
| cpe:2.3:a:joomla:joomla\!:3.4.1:rc2:*:*:*:*:*:* |
| cpe:2.3:a:joomla:joomla\!:3.4.2:*:*:*:*:*:*:* |
| cpe:2.3:a:joomla:joomla\!:3.4.2:rc1:*:*:*:*:*:* |
| cpe:2.3:a:joomla:joomla\!:3.4.3:*:*:*:*:*:*:* |

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→