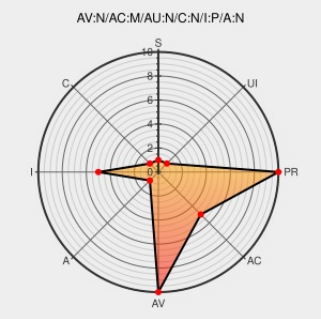
# CVE-2012-0047

Published on: 03/23/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:23 PM UTC

## CVE-2012-0047

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




Certain versions of Wicket from Apache contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in Apache Wicket 1.4.x before 1.4.20 allows remote attackers to inject arbitrary web script or HTML via the wicket:pageMapName parameter.

CVE-2012-0047 has been assigned by secalert@redhat.com 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 |
|---|---|---|
| Apache Wicket Input Validation Flaw in 'wicket:pageMapName' Parameter Permits Cross-Site Scripting Attacks - SecurityTracker | www.securitytracker.com text/html | SECTRACK 1026839 |
| No Description Provided | osvdb.org Inactive Link Not Archived | OSVDB 80300 |
| IBM X-Force Exchange | exchange.xforce.ibmcloud.com text/html | XF apache-wicket-unspec-xss(74273) |
| No Description Provided | archives.neohapsis.com Inactive Link Not Archived | BUGTRAQ 20120322 [CVE-2012-0047] Apache Wicket XSS vulnerability via pageMapName request parameter |
| Apache Wicket - CVE-2012-0047 - Apache Wicket XSS vulnerability via pageMapName request parameter | Vendor Advisory web.archive.org | CONFIRM wicket.apache.org/2012/03/22/wicket-cve- |

text/html
Inactive Link Not Archived

2012-0047.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 |
|---|---|---|---|---|---|---|
| Application | Apache | Wicket | 1.4.0 | All | All | All |
| Application | Apache | Wicket | 1.4.1 | All | All | All |
| Application | Apache | Wicket | 1.4.10 | All | All | All |
| Application | Apache | Wicket | 1.4.11 | All | All | All |
| Application | Apache | Wicket | 1.4.12 | All | All | All |
| Application | Apache | Wicket | 1.4.13 | All | All | All |
| Application | Apache | Wicket | 1.4.14 | All | All | All |
| Application | Apache | Wicket | 1.4.15 | All | All | All |
| Application | Apache | Wicket | 1.4.16 | All | All | All |
| Application | Apache | Wicket | 1.4.17 | All | All | All |
| Application | Apache | Wicket | 1.4.18 | All | All | All |
| Application | Apache | Wicket | 1.4.19 | All | All | All |
| Application | Apache | Wicket | 1.4.2 | All | All | All |
| Application | Apache | Wicket | 1.4.3 | All | All | All |
| Application | Apache | Wicket | 1.4.4 | All | All | All |
| Application | Apache | Wicket | 1.4.5 | All | All | All |
| Application | Apache | Wicket | 1.4.6 | All | All | All |
| Application | Apache | Wicket | 1.4.7 | All | All | All |
| Application | Apache | Wicket | 1.4.8 | All | All | All |
| Application | Apache | Wicket | 1.4.9 | All | All | All |
| Application | Apache | Wicket | 1.4.0 | All | All | All |
| Application | Apache | Wicket | 1.4.1 | All | All | All |
| Application | Apache | Wicket | 1.4.10 | All | All | All |
| Application | Apache | Wicket | 1.4.11 | All | All | All |
| Application | Apache | Wicket | 1.4.12 | All | All | All |
| Application | Apache | Wicket | 1.4.13 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Apache | Wicket | 1.4.14 | All | All | All |
| Application | Apache | Wicket | 1.4.15 | All | All | All |
| Application | Apache | Wicket | 1.4.16 | All | All | All |
| Application | Apache | Wicket | 1.4.17 | All | All | All |
| Application | Apache | Wicket | 1.4.18 | All | All | All |
| Application | Apache | Wicket | 1.4.19 | All | All | All |
| Application | Apache | Wicket | 1.4.2 | All | All | All |
| Application | Apache | Wicket | 1.4.3 | All | All | All |
| Application | Apache | Wicket | 1.4.4 | All | All | All |
| Application | Apache | Wicket | 1.4.5 | All | All | All |
| Application | Apache | Wicket | 1.4.6 | All | All | All |
| Application | Apache | Wicket | 1.4.7 | All | All | All |
| Application | Apache | Wicket | 1.4.8 | All | All | All |
| Application | Apache | Wicket | 1.4.9 | All | All | All |

cpe:2.3:a:apache:wicket:1.4.0:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.1:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.10:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.11:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.12:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.13:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.14:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.15:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.16:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.17:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.18:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.19:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.2:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.3:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.4:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.5:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.6:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.7:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.8:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.9:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.0:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.1:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.10:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.11:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.12:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.13:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.14:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.15:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.16:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.17:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.18:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.19:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.2:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.3:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.4:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.5:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.6:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.7:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.8:*:*:*:*:*:*:*

cpe:2.3:a:apache:wicket:1.4.9:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status status.cve.report**