



CVE-2015-5210

Published on: 11/02/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:14 PM UTC

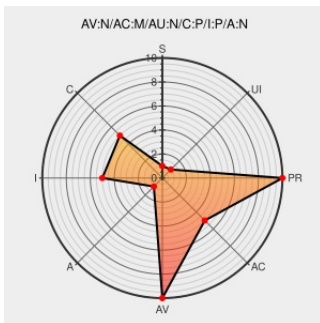
CVE-2015-5210

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Ambari](#) from [Apache](#) contain the following vulnerability:

Open redirect vulnerability in Apache Ambari before 2.1.2 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the targetURI parameter.

CVE-2015-5210 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Ambari Vulnerabilities - Apache Ambari -
Apache Software Foundation

[Vendor Advisory](#)
[cwiki.apache.org](http://cwiki.apache.org/text/html)
[text/html](#)

CONFIRM
cwiki.apache.org/confluence/display/AMBARI/Ambari+Vulnerabilities

oss-security - [CVE-2015-5210] Unvalidated
Redirects and Forwards using targetURI
parameter can enable phishing exploits

[www.openwall.com](http://www.openwall.com/text/html)
[text/html](#)

**MLIST [oss-security] 20151013 [CVE-2015-5210] Unvalidated
Redirects and Forwards using targetURI parameter can enable
phishing exploits**

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.

Related QID Numbers

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Ambari	1.7.0	All	All	All
Application	Apache	Ambari	2.0.0	All	All	All
Application	Apache	Ambari	2.0.1	All	All	All
Application	Apache	Ambari	2.0.2	All	All	All
Application	Apache	Ambari	2.1.0	All	All	All
Application	Apache	Ambari	1.7.0	All	All	All
Application	Apache	Ambari	2.0.0	All	All	All
Application	Apache	Ambari	2.0.1	All	All	All
Application	Apache	Ambari	2.0.2	All	All	All
Application	Apache	Ambari	2.1.0	All	All	All
Application	Apache	Ambari	All	All	All	All

```
cpe:2.3:a:apache:ambari:1.7.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:ambari:2.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:ambari:2.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:ambari:2.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:ambari:2.1.0:*:*:*:*:*:
```

```
cpe:2.3:a:apache:ambari:1.7.0:*:*:*:*:*:
```

```
cpe:2.3:a:apache:ambari:2.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:ambari:2.0.1:*.:*:*:*:*:
```

```
cpe:2.3:a:apache:ambari:2.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:ambari:2.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:ambari:*:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

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](#)