



# CVE-2022-36905

Published on: Not Yet Published

Last Modified on: 10/25/2023 06:17:00 PM UTC

## CVE-2022-36905

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Maven Metadata](#) from [Jenkins](#) contain the following vulnerability:

Jenkins Maven Metadata Plugin for Jenkins CI server Plugin 2.2 and earlier does not perform URL validation for the Repository Base URL of List maven artifact versions parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.

CVE-2022-36905 has been assigned by [jenkinsci-cert@googlegroups.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Jenkins project](#) - **Jenkins Maven Metadata Plugin for Jenkins CI server Plugin** version **not down converted**

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>         |

## CVE References

| Description                                                | Tags                                                          | Link                                                                                      |
|------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| oss-security - Multiple vulnerabilities in Jenkins plugins | <a href="#">www.openwall.com</a><br><a href="#">text/html</a> | <a href="#">MLIST [oss-security] 20220727 Multiple vulnerabilities in Jenkins plugins</a> |
| Jenkins Security Advisory 2022-07-27                       | <a href="#">www.jenkins.io</a><br><a href="#">text/html</a>   | <a href="#">CONFIRM www.jenkins.io/security/advisory/2022-07-27/#SECURITY-2686</a>        |

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                                             | <a href="#">Jenkins</a> | <a href="#">Maven Metadata</a> | All     | All    | All     | All      |
| cpe:2.3:a:jenkins:maven_metadata:*:*:*:*:jenkins_ci:*:* |                         |                                |         |        |         |          |

No vendor comments have been submitted for this CVE

#### Social Mentions

| Source                                                                                       | Title                                                                                                                                                                                                    | Posted (UTC)           |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
|  @CVEreport  | CVE-2022-36905 : Jenkins Maven Metadata Plugin for Jenkins CI server Plugin 2.2 and earlier does not perform URL va... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-07-27<br>14:45:23 |
|  @LinInfoSec | Jenkins - CVE-2022-36905: <a href="https://jenkins.io/security/advis...">jenkins.io/security/advis...</a>                                                                                                | 2022-07-27<br>18:03:31 |
|  /r/netcve  | <a href="#">CVE-2022-36905</a>                                                                                                                                                                           | 2022-07-27<br>15:38:25 |

[← 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](#)