tenable Nessus

Report generated by Tenable Nessus™

shopcart

Wed, 13 Nov 2024 19:54:06 +03

TABLE OF CONTENTS

Vulnerabilities by Host

- 13.52.135.157

Vulnerabilities by Host

Collapse All | Expand All

13.52.135.157

4	15	11	0	28
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

DNS Name:	ec2-13-52-135-157.us-west-1.compute.amazonaws.com
IP:	13.52.135.157
OS:	Linux Kernel 2.6

Vulnerabilities

154894 - Jenkins LTS < 2.303.3 / Jenkins weekly < 2.319 Multiple Vulnerabilities -

Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.303.3 or Jenkins weekly prior to 2.319. It is, therefore, affected by multiple vulnerabilities:

- Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not check agent-to-controller access to create parent directories in FilePath#mkdirs. (CVE-2021-21685)

- File path filters in the agent-to-controller security subsystem of Jenkins 2.318 and earlier, LTS 2.303.2 and earlier do not canonicalize paths, allowing operations to follow symbolic links to outside allowed directories. (CVE-2021-21686)

- Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not check agent-to-controller access to create symbolic links when unarchiving a symbolic link in FilePath#untar. (CVE-2021-21687)

- The agent-to-controller security check FilePath#reading(FileVisitor) in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not reject any operations, allowing users to have unrestricted read access using certain operations (creating archives, FilePath#copyRecursiveTo). (CVE-2021-21688)

- FilePath#unzip and FilePath#untar were not subject to any agent-to-controller access control in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier. (CVE-2021-21689)

- Agent processes are able to completely bypass file path filtering by wrapping the file operation in an agent file path in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier. (CVE-2021-21690)

- Creating symbolic links is possible without the 'symlink' agent-to-controller access control permission in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier. (CVE-2021-21691)

- FilePath#renameTo and FilePath#moveAllChildrenTo in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier only check 'read' agent-to-controller access permission on the source path, instead of 'delete'.
(CVE-2021-21692)

- When creating temporary files, agent-to-controller access to create those files is only checked after they've been created in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier. (CVE-2021-21693)

- FilePath#toURI, FilePath#hasSymlink, FilePath#absolutize, FilePath#isDescendant, and FilePath#get*DiskSpace do not check any permissions in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier.
(CVE-2021-21694)

- FilePath#listFiles lists files outside directories that agents are allowed to access when following symbolic links in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier. (CVE-2021-21695)

- Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not limit agent read/write access to the libs/ directory inside build directories when using the FilePath APIs, allowing attackers in control of agent processes to replace the code of a trusted library with a modified variant. This results in unsandboxed code execution in the Jenkins controller process. (CVE-2021-21696)

- Jenkins 2.318 and earlier, LTS 2.303.2 and earlier allows any agent to read and write the contents of any build directory stored in Jenkins with very few restrictions. (CVE-2021-21697)

- Jenkins Subversion Plugin 2.15.0 and earlier does not restrict the name of a file when looking up a subversion key file on the controller from an agent. (CVE-2021-21698)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2021-11-04

Solution

Upgrade Jenkins weekly to version 2.319 or later or Jenkins LTS to version 2.303.3 or later

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-21685
CVE	CVE-2021-21686
CVE	CVE-2021-21687
CVE	CVE-2021-21688
CVE	CVE-2021-21689
CVE	CVE-2021-21690
CVE	CVE-2021-21691

CVE	CVE-2021-21692
CVE	CVE-2021-21693
CVE	CVE-2021-21694
CVE	CVE-2021-21695
CVE	CVE-2021-21696
CVE	CVE-2021-21697
CVE	CVE-2021-21698
XREF	IAVA:2021-A-0551-S

Plugin Information

Published: 2021/11/04, Modified: 2024/06/04

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.303.3
```

163258 - Jenkins LTS < 2.332.4 / Jenkins weekly < 2.356 Multiple Vulnerabilities -

Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.332.4 or Jenkins weekly prior to 2.356. It is, therefore, affected by multiple vulnerabilities:

- Multiple cross-site scripting (XSS) vulnerabilities in Jenkins 2.355 and earlier, LTS 2.332.3 and earlier allow attackers to inject HTML and JavaScript into the Jenkins UI: SECURITY-2779 (CVE-2022-34170): Since Jenkins 2.320 and LTS 2.332.1, help icon tooltips no longer escape the feature name, effectively undoing the fix for SECURITY-1955. SECURITY-2761 (CVE-2022-34171): Since Jenkins 2.321 and LTS 2.332.1, the HTML output generated for new symbol-based SVG icons includes the title attribute of l:ionicon until Jenkins 2.334 and alt attribute of l:icon since Jenkins 2.335 without further escaping. SECURITY-2776 (CVE-2022-34172): Since Jenkins 2.340, symbol-based icons unescape previously escaped values of tooltip parameters. SECURITY-2780 (CVE-2022-34173): Since Jenkins 2.340, the tooltip of the build button in list views supports HTML without escaping the job display name. These vulnerabilities are known to be exploitable by attackers with Job/Configure permission. Jenkins 2.356, LTS 2.332.4 and LTS 2.346.1 addresses these vulnerabilities: SECURITY-2779: The feature name in help icon tooltips is now escaped. SECURITY-2761: The title attribute of l:ionicon (Jenkins LTS 2.332.4) and alt attribute of l:icon (Jenkins 2.356 and LTS 2.346.1) are escaped in the generated HTML output. SECURITY-2776: Symbol-based icons no longer unescape values of tooltip parameters. SECURITY-2780: The tooltip of the build button in list views is now escaped. No Jenkins LTS release is affected by SECURITY-2776 or SECURITY-2780, as these were not present in Jenkins 2.332.x and fixed in the 2.346.x line before 2.346.1. (CVE-2022-34170, CVE-2022-34171, CVE-2022-34172, CVE-2022-34173)

- In Jenkins 2.355 and earlier, LTS 2.332.3 and earlier, an observable timing discrepancy on the login form allows distinguishing between login attempts with an invalid username, and login attempts with a valid username and wrong password, when using the Jenkins user database security realm. This allows attackers to determine the validity of attacker-specified usernames. Login attempts with an invalid username now validate a synthetic password to eliminate the timing discrepancy in Jenkins 2.356, LTS 2.332.4.
(CVE-2022-34174)

- Jenkins uses the Stapler web framework to render its UI views. These views are frequently composed of several view fragments, enabling plugins to extend existing views with more content. Before SECURITY-534 was fixed in Jenkins 2.186 and LTS 2.176.2, attackers could in some cases directly access a view fragment containing sensitive information, bypassing any permission checks in the corresponding view. In Jenkins 2.335 through 2.355 (both inclusive), the protection added for SECURITY-534 is disabled for some views. As a result, attackers could in very limited cases directly access a view fragment containing sensitive information, bypassing any permission checks in the corresponding view. As of publication, the Jenkins security team is unaware of any vulnerable view fragment across the Jenkins plugin ecosystem. Jenkins 2.356 restores the protection for affected views. (CVE-2022-34175)

- JUnit Plugin 1119.va_a_5e9068da_d7 and earlier does not escape descriptions of test results. This results in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Run/Update permission.
JUnit Plugin 1119.1121.vc43d0fc45561 applies the configured markup formatter to descriptions of test results. (CVE-2022-34176)

- Pipeline: Input Step Plugin 448.v37cea_9a_10a_70 and earlier allows Pipeline authors to specify file parameters for Pipeline input steps even though they are unsupported. Although the uploaded file is not copied to the workspace, Jenkins archives the file on the controller as part of build metadata using the parameter name without sanitization as a relative path inside a build-related directory. This allows attackers able to configure Pipelines to create or replace arbitrary files on the Jenkins controller file system with attacker-specified content. Pipeline: Input Step Plugin 449.v77f0e8b_845c4 prohibits use of file parameters for Pipeline input steps. Attempts to use them will fail Pipeline execution.
(CVE-2022-34177)

- Embeddable Build Status Plugin 2.0.3 allows specifying a link query parameter that build status badges will link to, without restricting possible values. This results in a reflected cross-site scripting (XSS) vulnerability. Embeddable Build Status Plugin 2.0.4 limits URLs to http and https protocols and correctly escapes the provided value. (CVE-2022-34178)

- Embeddable Build Status Plugin 2.0.3 and earlier allows specifying a style query parameter that is used to choose a different SVG image style without restricting possible values. This results in a relative path traversal vulnerability, allowing attackers without Overall/Read permission to specify paths to other SVG images on the Jenkins controller file system. Embeddable Build Status Plugin 2.0.4 restricts the style query parameter to one of the three legal values. (CVE-2022-34179)

- Embeddable Build Status Plugin 2.0.3 and earlier does not correctly perform the ViewStatus permission check in the HTTP endpoint it provides for unprotected status badge access. This allows attackers without any permissions to obtain the build status badge icon for any attacker-specified job and/or build.
Embeddable Build Status Plugin 2.0.4 requires ViewStatus permission to obtain the build status badge icon.
(CVE-2022-34180)

- xUnit Plugin 3.0.8 and earlier implements an agent-to-controller message that creates a user-specified directory if it doesn't exist, and parsing files inside it as test results. This allows attackers able to control agent processes to create an arbitrary directory on the Jenkins controller or to obtain test results from existing files in an attacker-specified directory. xUnit Plugin 3.1.0 changes the message type from agent-to-controller to controller-to-agent, preventing execution on the controller.
(CVE-2022-34181)

- Nested View Plugin 1.20 through 1.25 (both inclusive) does not escape search parameters. This results in a reflected cross-site scripting (XSS) vulnerability. Nested View Plugin 1.26 escapes search parameters.
(CVE-2022-34182)

- Multiple plugins do not escape the name and description of the parameter types they provide: Agent Server Parameter 1.1 and earlier (SECURITY-2731 / CVE-2022-34183) CRX Content Package Deployer 1.9 and earlier (SECURITY-2727 / CVE-2022-34184) Date Parameter Plugin 0.0.4 and earlier (SECURITY-2711 / CVE-2022-34185) Dynamic Extended Choice Parameter 1.0.1 and earlier (SECURITY-2712 / CVE-2022-34186) Filesystem List Parameter 0.0.7 and earlier (SECURITY-2716 / CVE-2022-34187) Hidden Parameter Plugin 0.0.4 and earlier (SECURITY-2755 / CVE-2022-34188) Image Tag Parameter 1.10 and earlier (SECURITY-2721 / CVE-2022-34189) Maven Metadata for CI server 2.1 and earlier (SECURITY-2714 / CVE-2022-34190) NS-ND Integration Performance Publisher 4.8.0.77 and earlier (SECURITY-2736 / CVE-2022-34191) ontrack Jenkins 4.0.0 and earlier (SECURITY-2733 / CVE-2022-34192) Package Version 1.0.1 and earlier (SECURITY-2735 / CVE-2022-34193) Readonly Parameter 1.0.0 and earlier (SECURITY-2719 / CVE-2022-34194) Repository Connector 2.2.0 and earlier (SECURITY-2666 / CVE-2022-34195) REST List Parameter Plugin 1.5.2 and earlier (SECURITY-2730 / CVE-2022-34196) Sauce OnDemand 1.204 and earlier (SECURITY-2724 / CVE-2022-34197) Stash Branch Parameter 0.3.0 and earlier (SECURITY-2725 / CVE-2022-34198) This results in stored cross-site scripting (XSS) vulnerabilites exploitable by attackers with Item/Configure permission. Exploitation of these vulnerabilities requires that parameters are listed on another page, like the Build With Parameters and Parameters pages provided by Jenkins (core), and that those pages are not hardened to prevent exploitation. Jenkins (core) has prevented exploitation of vulnerabilities of this kind on the Build With Parameters and Parameters pages since 2.44 and LTS 2.32.2 as part of the SECURITY-353 / CVE-2017-2601 fix. Additionally, several plugins have previously been updated to list parameters in a way that prevents exploitation by default, see SECURITY-2617 in the 2022-04-12 security advisory for a list.
The following plugins have been updated to escape the name and description of the parameter types they provide in the versions specified: REST List Parameter Plugin 1.6.0 Hidden Parameter Plugin 0.0.5 As of publication of this advisory, there is no fix available for the following plugins: Agent Server Parameter 1.1 and earlier (SECURITY-2731 / CVE-2022-34183) CRX Content Package Deployer 1.9 and earlier (SECURITY-2727 / CVE-2022-34184) Date Parameter Plugin 0.0.4 and earlier (SECURITY-2711 / CVE-2022-34185) Dynamic Extended Choice Parameter 1.0.1 and earlier (SECURITY-2712 / CVE-2022-34186) Filesystem List Parameter 0.0.7 and earlier (SECURITY-2716 / CVE-2022-34187) Image Tag Parameter 1.10 and earlier (SECURITY-2721 / CVE-2022-34189) Maven Metadata for CI server 2.1 and earlier (SECURITY-2714 / CVE-2022-34190) NS-ND Integration Performance Publisher 4.8.0.77 and earlier (SECURITY-2736 / CVE-2022-34191) ontrack Jenkins 4.0.0 and earlier (SECURITY-2733 / CVE-2022-34192) Package Version 1.0.1 and earlier (SECURITY-2735 / CVE-2022-34193) Readonly Parameter 1.0.0 and earlier (SECURITY-2719 / CVE-2022-34194) Repository Connector 2.2.0 and earlier (SECURITY-2666 / CVE-2022-34195) Sauce OnDemand 1.204 and earlier (SECURITY-2724 / CVE-2022-34197) Stash Branch Parameter 0.3.0 and earlier (SECURITY-2725 / CVE-2022-34198) (CVE-2022-34183, CVE-2022-34184, CVE-2022-34185, CVE-2022-34186, CVE-2022-34187, CVE-2022-34188, CVE-2022-34189, CVE-2022-34190, CVE-2022-34191, CVE-2022-34192, CVE-2022-34193, CVE-2022-34194, CVE-2022-34195, CVE-2022-34196, CVE-2022-34197, CVE-2022-34198)

- Convertigo Mobile Platform Plugin 1.1 and earlier stores passwords unencrypted in job config.xml files on the Jenkins controller as part of its configuration. These passwords can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system. As of publication of this advisory, there is no fix. (CVE-2022-34199)

- Convertigo Mobile Platform Plugin 1.1 and earlier does not perform a permission check in a method implementing form validation. This allows attackers with Overall/Read permission to connect to an attacker-specified URL. Additionally, this form validation method does not require POST requests, resulting in a cross-site request forgery (CSRF) vulnerability. As of publication of this advisory, there is no fix. (CVE-2022-34200, CVE-2022-34201)

- EasyQA Plugin 1.0 and earlier stores user passwords unencrypted in its global configuration file EasyQAPluginProperties.xml on the Jenkins controller as part of its configuration. These passwords can be viewed by users with access to the Jenkins controller file system. As of publication of this advisory, there is no fix.
(CVE-2022-34202)

- EasyQA Plugin 1.0 and earlier does not perform a permission check in a method implementing form validation. This allows attackers with Overall/Read permission to connect to an attacker-specified HTTP server. Additionally, this form validation method does not require POST requests, resulting in a cross- site request forgery (CSRF) vulnerability. As of publication of this advisory, there is no fix.
(CVE-2022-34203, CVE-2022-34204)

- Jianliao Notification Plugin 1.1 and earlier does not perform a permission check in a method implementing form validation. This allows attackers with Overall/Read permission to send HTTP POST requests to an attacker-specified URL. Additionally, this form validation method does not require POST requests, resulting in a cross-site request forgery (CSRF) vulnerability. As of publication of this advisory, there is no fix. (CVE-2022-34205, CVE-2022-34206)

- Beaker builder Plugin 1.10 and earlier does not perform a permission check in a method implementing form validation. This allows attackers with Overall/Read permission to connect to an attacker-specified URL.
Additionally, this form validation method does not require POST requests, resulting in a cross-site request forgery (CSRF) vulnerability. As of publication of this advisory, there is no fix.
(CVE-2022-34207, CVE-2022-34208)

- ThreadFix Plugin 1.5.4 and earlier does not perform a permission check in a method implementing form validation. This allows attackers with Overall/Read permission to connect to an attacker-specified URL.
Additionally, this form validation method does not require POST requests, resulting in a cross-site request forgery (CSRF) vulnerability. As of publication of this advisory, there is no fix.
(CVE-2022-34209, CVE-2022-34210)

- vRealize Orchestrator Plugin 3.0 and earlier does not perform a permission check in an HTTP endpoint. This allows attackers with Overall/Read permission to send an HTTP POST request to an attacker-specified URL.
Additionally, this HTTP endpoint does not require POST requests, resulting in a cross-site request forgery (CSRF) vulnerability. As of publication of this advisory, there is no fix. (CVE-2022-34211, CVE-2022-34212)

- Squash TM Publisher (Squash4Jenkins) Plugin 1.0.0 and earlier stores passwords unencrypted in its global configuration file org.jenkinsci.squashtm.core.SquashTMPublisher.xml on the Jenkins controller as part of its configuration. These passwords can be viewed by users with access to the Jenkins controller file system. As of publication of this advisory, there is no fix. (CVE-2022-34213)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2022-06-22

Solution

Upgrade Jenkins weekly to version 2.356 or later or Jenkins LTS to version 2.332.4, 2.346.1, or later

Risk Factor

Medium

CVSS v3.0 Base Score

9.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2022-34170
CVE	CVE-2022-34171
CVE	CVE-2022-34172
CVE	CVE-2022-34173
CVE	CVE-2022-34174
CVE	CVE-2022-34175
CVE	CVE-2022-34176
CVE	CVE-2022-34177
CVE	CVE-2022-34178
CVE	CVE-2022-34179
CVE	CVE-2022-34180
CVE	CVE-2022-34181
CVE	CVE-2022-34182
CVE	CVE-2022-34183
CVE	CVE-2022-34184
CVE	CVE-2022-34185
CVE	CVE-2022-34186
CVE	CVE-2022-34187

CVE	CVE-2022-34188
CVE	CVE-2022-34189
CVE	CVE-2022-34190
CVE	CVE-2022-34191
CVE	CVE-2022-34192
CVE	CVE-2022-34193
CVE	CVE-2022-34194
CVE	CVE-2022-34195
CVE	CVE-2022-34196
CVE	CVE-2022-34197
CVE	CVE-2022-34198
CVE	CVE-2022-34199
CVE	CVE-2022-34200
CVE	CVE-2022-34201
CVE	CVE-2022-34202
CVE	CVE-2022-34203
CVE	CVE-2022-34204
CVE	CVE-2022-34205
CVE	CVE-2022-34206
CVE	CVE-2022-34207
CVE	CVE-2022-34208
CVE	CVE-2022-34209
CVE	CVE-2022-34210
CVE	CVE-2022-34211
CVE	CVE-2022-34212
CVE	CVE-2022-34213

Plugin Information

Published: 2022/07/15, Modified: 2024/06/04

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.332.4 or 2.346.1
```

172394 - Jenkins LTS < 2.375.4 / Jenkins weekly < 2.394 Multiple Vulnerabilities +

189463 - Jenkins LTS < 2.426.3 / Jenkins weekly < 2.442 Multiple Vulnerabilities -

Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.426.3 or Jenkins weekly prior to 2.442. It is, therefore, affected by multiple vulnerabilities:

- Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system. (CVE-2024-23897)

- Jenkins 2.217 through 2.441 (both inclusive), LTS 2.222.1 through 2.426.2 (both inclusive) does not perform origin validation of requests made through the CLI WebSocket endpoint, resulting in a cross-site WebSocket hijacking (CSWSH) vulnerability, allowing attackers to execute CLI commands on the Jenkins controller. (CVE-2024-23898)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2024-01-24

Solution

Upgrade Jenkins weekly to version 2.442 or later, or Jenkins LTS to version 2.426.3 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2024-23897
CVE	CVE-2024-23898
XREF	JENKINS:2024-01-24
XREF	IAVA:2024-A-0057-S
XREF	CISA-KNOWN-EXPLOITED:2024/09/09

Exploitable With

Core Impact (true)

Plugin Information

Published: 2024/01/24, Modified: 2024/08/19

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.426.3
```

135178 - Jenkins < (2.204.6 / 2.222.1) LTS / 2.228 Multiple Vulnerabilities -

Synopsis

A job scheduling and management system hosted on the remote web server is affected by multiple vulnerabilities.

Description

The version of Jenkins running on the remote web server is prior to 2.228 or is a version of Jenkins LTS prior to 2.204.6 or 2.222.1. It is, therefore, affected by multiple vulnerabilities:

- An authentication bypass vulnerability exists in Jenkins' CSRF prevention component. An unauthenticated, remote attacker can exploit this, by sending specially crafted requests to a vulnerable Jenkins instance, to bypass authentication and conduct a CSRF attack (CVE-2020-2160).

- A stored cross-site scripting (XSS) vulnerability exists in Jenkins' label expression validation component due to improper validation of user-supplied input before returning it to users. An authenticated, remote attacker can exploit this, by convincing a user to click a specially crafted URL, to execute arbitrary script code in a user's browser session (CVE-2020-2161).

- A stored cross-site scripting (XSS) vulnerability exists in Jenkins' file parameter component due to improper validation of user-supplied input before returning it to users. An authenticated, remote attacker can exploit this, by convincing a user to click a specially crafted URL, to execute arbitrary script code in a user's browser session (CVE-2020-2162).

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?edd15de3

Solution

Upgrade Jenkins to version 2.228 or later. Upgrade Jenkins LTS to version 2.204.6, 2.222.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2020-2160
CVE	CVE-2020-2161
CVE	CVE-2020-2162
CVE	CVE-2020-2163
XREF	IAVA:2020-A-0126-S

Plugin Information

Published: 2020/04/02, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.204.6 or 2.222.1 LTS / 2.228
```

124168 - Jenkins < 2.164.2 LTS / 2.172 Multiple Vulnerabilities -

Synopsis

A job scheduling and management system hosted on the remote web server is affected by multiple vulnerabilities.

Description

The version of Jenkins running on the remote web server is prior to 2.172 or is a version of Jenkins LTS prior to 2.164.2. It is, therefore, affected by multiple vulnerabilities:

- An authentication bypass condition exists due to an incomplete fix for SECURITY-901, in which existing remote-based CLI authentication caches. An unauthenticated, remote attacker can exploit this to bypass existing Access Control Limitations and appear as an authenticated user. (CVE-2019-1003049)

- A cross-site scripting (XSS) vulnerability exists due to improper validation of user-supplied input before returning it to users. An unauthenticated, remote attacker can exploit this, by convincing a user to click a specially crafted URL, to execute arbitrary script code in a user's browser session. (CVE-2019-1003050) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2019-04-10/

Solution

Upgrade Jenkins to version 2.172 or later, Jenkins LTS to version 2.164.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.1 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	107889
BID	107901
CVE	CVE-2019-1003049
CVE	CVE-2019-1003050

Plugin Information

Published: 2019/04/18, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.164.2 LTS / 2.172
```

127053 - Jenkins < 2.176.2 LTS / 2.186 Multiple Vulnerabilities -

Synopsis

A job scheduling and management system hosted on the remote web server is affected by multiple vulnerabilities.

Description

The version of Jenkins running on the remote web server is prior to 2.186 or is a version of Jenkins LTS prior to 2.176.2. It is, therefore, affected by multiple vulnerabilities:

- An arbitrary file write vulnerability exists due to an incomplete fix for SECURITY-1074, the improper validation of the file parameter definition. An authenticated, remote attacker can exploit this, via a file name with a relative path escaping the base directory, to write arbitrary files on the remote host. (CVE-2019-10352)

- A security bypass vulnerability exists due to insufficent validaiton of CSRF tokens. An unauthenticated, remote attacker can exploit this, after obtaining the CSRF token of another user, to bypass CSRF protections and implement a CSRF attack. (CVE-2019-10353)

- An information disclosure vulnerability exists in the Stapler web framework due to inadequit permission control of view fragments. An authenticated, remote attacker can exploit this, to disclose potentially sensitive information. (CVE-2019-10354)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2019-07-17/
https://www.tenable.com/security/research/tra-2019-35

Solution

Upgrade Jenkins to version 2.186 or later, Jenkins LTS to version 2.176.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

4.0 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	109299
BID	109373
CVE	CVE-2019-10352
CVE	CVE-2019-10353
CVE	CVE-2019-10354
XREF	TRA:TRA-2019-35

Plugin Information

Published: 2019/07/26, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.176.2 LTS / 2.186
```

129776 - Jenkins < 2.176.3 LTS / 2.192 Multiple Vulnerabilities -

Synopsis

A job scheduling and management system hosted on the remote web server is affected by multiple vulnerabilities.

Description

The version of Jenkins running on the remote web server is prior to 2.192 or is a version of Jenkins LTS prior to 2.176.3. It is, therefore, affected by multiple vulnerabilities:

- A stored Cross-site scripting (XSS) vulnerability exists in the Jenkins update center. An authenticated, remote attacker with Overall/Administer permission can exploit this by configuring the update site URL to inject arbitrary HTML and JavaScript in update center web pages. (CVE-2019-10383)

- A Cross-site request forgery (XSRF) vulnerability exists in Jenkins, caused by an incomplete fix for SECURITY-626. This allowed users to obtain CSRF tokens without an associated web session ID, resulting in CSRF tokens that did not expire. An unauthenticated, remote attacker can exploit this to bypass CSRF protections for the anonymous user. (CVE-2019-10384)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2019-08-28/

Solution

Upgrade Jenkins to version 2.192 or later, Jenkins LTS to version 2.176.3 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2019-10383
CVE	CVE-2019-10384

Plugin Information

Published: 2019/10/10, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.176.3 LTS / 2.192
```

145248 - Jenkins < 2.263.2 LTS / 2.275 Multiple Vulnerabilities -

Synopsis

A job scheduling and management system hosted on the remote web server is affected by multiple vulnerabilities.

Description

The version of Jenkins running on the remote web server is prior to 2.275 or is a version of Jenkins LTS prior to 2.263.2. It is, therefore, affected by multiple vulnerabilities, including the following:

- Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows users with Agent/Configure permission to choose agent names that cause Jenkins to override the global `config.xml` file. (CVE-2021-21605)

- Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows attackers with permission to create or configure various objects to inject crafted content into Old Data Monitor that results in the instantiation of potentially unsafe objects once discarded by an administrator. (CVE-2021-21604)

- Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not correctly match requested URLs to the list of always accessible paths, allowing attackers without Overall/Read permission to access some URLs as if they did have Overall/Read permission. (CVE-2021-21609)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://www.jenkins.io/security/advisory/2021-01-13/

Solution

Upgrade Jenkins to version 2.275 or later, Jenkins LTS to version 2.263.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

8.0 (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.0 (CVSS2#AV:N/AC:M/Au:S/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

4.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-21602
CVE	CVE-2021-21603
CVE	CVE-2021-21604
CVE	CVE-2021-21605
CVE	CVE-2021-21606
CVE	CVE-2021-21607
CVE	CVE-2021-21608
CVE	CVE-2021-21609
CVE	CVE-2021-21610
CVE	CVE-2021-21611
XREF	IAVA:2021-A-0039-S

Plugin Information

Published: 2021/01/22, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.263.2 LTS / 2.275
```

148975 - Jenkins LTS < 2.277.3 / Jenkins weekly < 2.286 -

Synopsis

An application running on a remote web server host is affected by a vulnerability

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.277.3 or Jenkins weekly prior to 2.286. It is, therefore, affected by a vulnerability:

- In Eclipse Jetty 7.2.2 to 9.4.38, 10.0.0.alpha0 to 10.0.1, and 11.0.0.alpha0 to 11.0.1, CPU usage can reach 100% upon receiving a large invalid TLS frame. (CVE-2021-28165)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2021-04-20

Solution

Upgrade Jenkins weekly to version 2.286 or later or Jenkins LTS to version 2.277.3 or later

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2021-28165

Plugin Information

Published: 2021/04/23, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.277.3
```

151193 - Jenkins LTS < 2.289.2 / Jenkins weekly < 2.300 Multiple Vulnerabilities -

Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.289.2 or Jenkins weekly prior to 2.300. It is, therefore, affected by multiple vulnerabilities:

- Jenkins 2.299 and earlier, LTS 2.289.1 and earlier allows users to cancel queue items and abort builds of jobs for which they have Item/Cancel permission even when they do not have Item/Read permission. Jenkins 2.300, LTS 2.289.2 requires that users have Item/Read permission for applicable types in addition to Item/Cancel permission. As a workaround on earlier versions of Jenkins, do not grant Item/Cancel permission to users who do not have Item/Read permission. (CVE-2021-21670)

- Jenkins 2.299 and earlier, LTS 2.289.1 and earlier does not invalidate the existing session on login. This allows attackers to use social engineering techniques to gain administrator access to Jenkins. This vulnerability was introduced in Jenkins 2.266 and LTS 2.277.1. Jenkins 2.300, LTS 2.289.2 invalidates the existing session on login. Note In case of problems, administrators can choose a different implementation by setting the Java system property hudson.security.SecurityRealm.sessionFixationProtectionMode to 2, or disable the fix entirely by setting that system property to 0. (CVE-2021-21671)

- Selenium HTML report Plugin 1.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. This allows attackers with the ability to control the report files parsed using this plugin to have Jenkins parse a crafted report file that uses external entities for extraction of secrets from the Jenkins controller or server-side request forgery. Selenium HTML report Plugin 1.1 disables external entity resolution for its XML parser. (CVE-2021-21672)

- CAS Plugin 1.6.0 and earlier improperly determines that a redirect URL after login is legitimately pointing to Jenkins. This allows attackers to perform phishing attacks by having users go to a Jenkins URL that will forward them to a different site after successful authentication. CAS Plugin 1.6.1 only redirects to relative (Jenkins) URLs. (CVE-2021-21673)

- requests-plugin Plugin 2.2.6 and earlier does not perform a permission check in an HTTP endpoint. This allows attackers with Overall/Read permission to view the list of pending requests. requests-plugin Plugin 2.2.7 requires Overall/Read permission to view the list of pending requests. (CVE-2021-21674)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2021-06-30

Solution

Upgrade Jenkins weekly to version 2.300 or later or Jenkins LTS to version 2.289.2 or later

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.3 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-21670
CVE	CVE-2021-21671
CVE	CVE-2021-21672
CVE	CVE-2021-21673
CVE	CVE-2021-21674
XREF	IAVA:2021-A-0335-S

Plugin Information

Published: 2021/06/30, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.289.2
```

156929 - Jenkins LTS < 2.319.2 / Jenkins weekly < 2.330 Multiple Vulnerabilities -

Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.319.2 or Jenkins weekly prior to 2.330. It is, therefore, affected by multiple vulnerabilities:

- A cross-site request forgery (CSRF) vulnerability in Jenkins 2.329 and earlier, LTS 2.319.1 and earlier allows attackers to trigger build of job without parameters

when no security realm is set.
(CVE-2022-20612)

- A cross-site request forgery (CSRF) vulnerability in Jenkins Mailer Plugin 391.ve4a_38c1b_cf4b_ and earlier allows attackers to use the DNS used by the Jenkins instance to resolve an attacker-specified hostname. (CVE-2022-20613)

- A missing permission check in Jenkins Mailer Plugin 391.ve4a_38c1b_cf4b_ and earlier allows attackers with Overall/Read access to use the DNS used by the Jenkins instance to resolve an attacker-specified hostname.
(CVE-2022-20614)

- Jenkins Matrix Project Plugin 1.19 and earlier does not escape HTML metacharacters in node and label names, and label descriptions, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Agent/Configure permission. (CVE-2022-20615)

- Jenkins Credentials Binding Plugin 1.27 and earlier does not perform a permission check in a method implementing form validation, allowing attackers with Overall/Read access to validate if a credential ID refers to a secret file credential and whether it's a zip file. (CVE-2022-20616)

- Jenkins Docker Commons Plugin 1.17 and earlier does not sanitize the name of an image or a tag, resulting in an OS command execution vulnerability exploitable by attackers with Item/Configure permission or able to control the contents of a previously configured job's SCM repository. (CVE-2022-20617)

- A missing permission check in Jenkins Bitbucket Branch Source Plugin 737.vdf9dc06105be and earlier allows attackers with Overall/Read access to enumerate credentials IDs of credentials stored in Jenkins.
(CVE-2022-20618)

- A cross-site request forgery (CSRF) vulnerability in Jenkins Bitbucket Branch Source Plugin 737.vdf9dc06105be and earlier allows attackers to connect to an attacker-specified URL using attacker- specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.
(CVE-2022-20619)

- Missing permission checks in Jenkins SSH Agent Plugin 1.23 and earlier allows attackers with Overall/Read access to enumerate credentials IDs of credentials stored in Jenkins. (CVE-2022-20620)

- Jenkins Metrics Plugin 4.0.2.8 and earlier stores an access key unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system. (CVE-2022-20621)

- Jenkins Active Directory Plugin 2.25 and earlier does not encrypt the transmission of data between the Jenkins controller and Active Directory servers in most configurations. (CVE-2022-23105)

- Jenkins Configuration as Code Plugin 1.55 and earlier used a non-constant time comparison function when validating an authentication token allowing attackers to use statistical methods to obtain a valid authentication token. (CVE-2022-23106)

- Jenkins Warnings Next Generation Plugin 9.10.2 and earlier does not restrict the name of a file when configuring custom ID, allowing attackers with Item/Configure permission to write and read specific files with a hard-coded suffix on the Jenkins controller file system. (CVE-2022-23107)

- Jenkins Badge Plugin 1.9 and earlier does not escape the description and does not check for allowed protocols when creating a badge, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission. (CVE-2022-23108)

- Jenkins HashiCorp Vault Plugin 3.7.0 and earlier does not mask Vault credentials in Pipeline build logs or in Pipeline step descriptions when Pipeline: Groovy Plugin 2.85 or later is installed. (CVE-2022-23109)

- Jenkins Publish Over SSH Plugin 1.22 and earlier does not escape the SSH server name, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Overall/Administer permission. (CVE-2022-23110)

- A cross-site request forgery (CSRF) vulnerability in Jenkins Publish Over SSH Plugin 1.22 and earlier allows attackers to connect to an attacker-specified SSH server using attacker-specified credentials.
(CVE-2022-23111)

- A missing permission check in Jenkins Publish Over SSH Plugin 1.22 and earlier allows attackers with Overall/Read access to connect to an attacker-specified SSH server using attacker-specified credentials.
(CVE-2022-23112)

- Jenkins Publish Over SSH Plugin 1.22 and earlier performs a validation of the file name specifying whether it is present or not, resulting in a path traversal vulnerability allowing attackers with Item/Configure permission to discover the name of the Jenkins controller files. (CVE-2022-23113)

- Jenkins Publish Over SSH Plugin 1.22 and earlier stores password unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system. (CVE-2022-23114)

- Cross-site request forgery (CSRF) vulnerabilities in Jenkins batch task Plugin 1.19 and earlier allows attackers with Overall/Read access to retrieve logs, build or delete a batch task. (CVE-2022-23115)

- Jenkins Conjur Secrets Plugin 1.0.9 and earlier implements functionality that allows attackers able to control agent processes to decrypt secrets stored in Jenkins obtained through another method.
(CVE-2022-23116)

- Jenkins Conjur Secrets Plugin 1.0.9 and earlier implements functionality that allows attackers able to control agent processes to retrieve all username/password credentials stored on the Jenkins controller.
(CVE-2022-23117)

- Jenkins Debian Package Builder Plugin 1.6.11 and earlier implements functionality that allows agents to invoke command-line `git` at an attacker-specified path on the controller, allowing attackers able to control agent processes to invoke arbitrary OS commands on the controller. (CVE-2022-23118)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2022-01-12

Solution

Upgrade Jenkins weekly to version 2.330 or later or Jenkins LTS to version 2.319.2 or later

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-20612
CVE	CVE-2022-20613
CVE	CVE-2022-20614
CVE	CVE-2022-20615
CVE	CVE-2022-20616
CVE	CVE-2022-20617
CVE	CVE-2022-20618
CVE	CVE-2022-20619
CVE	CVE-2022-20620
CVE	CVE-2022-20621
CVE	CVE-2022-23105
CVE	CVE-2022-23106
CVE	CVE-2022-23107
CVE	CVE-2022-23108
CVE	CVE-2022-23109
CVE	CVE-2022-23110
CVE	CVE-2022-23111
CVE	CVE-2022-23112
CVE	CVE-2022-23113
CVE	CVE-2022-23114
CVE	CVE-2022-23115
CVE	CVE-2022-23116
CVE	CVE-2022-23117
CVE	CVE-2022-23118
XREF	IAVA:2022-A-0027-S
XREF	IAVA:2022-A-0084-S

Plugin Information

Published: 2022/01/21, Modified: 2024/06/04

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.319.2
```

157860 - Jenkins LTS < 2.319.3 / Jenkins weekly < 2.334 Multiple Vulnerabilities -

Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.319.3 or Jenkins weekly prior to 2.334. It is, therefore, affected by multiple vulnerabilities:

- XStream is an open source java library to serialize objects to XML and back again. Versions prior to 1.4.19 may allow a remote attacker to allocate 100% CPU time on the target system depending on CPU type or parallel execution of such a payload resulting in a denial of service only by manipulating the processed input stream. XStream 1.4.19 monitors and accumulates the time it takes to add elements to collections and throws an exception if a set threshold is exceeded. Users are advised to upgrade as soon as possible.
Users unable to upgrade may set the NO_REFERENCE mode to prevent recursion. See GHSA-rmr5-cpv2-vgjf for further details on a workaround if an upgrade is not possible. (CVE-2021-43859)

- Jenkins 2.333 and earlier, LTS 2.319.2 and earlier defines custom XStream converters that have not been updated to apply the protections for the vulnerability CVE-2021-43859 and allow unconstrained resource usage. (CVE-2022-0538)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2022-02-09

Solution

Upgrade Jenkins weekly to version 2.334 or later or Jenkins LTS to version 2.319.3 or later

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:C)

References

CVE	CVE-2021-43859
CVE	CVE-2022-0538

Plugin Information

Published: 2022/02/09, Modified: 2024/06/04

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.319.3
```

164898 - Jenkins LTS < 2.361.1 / Jenkins weekly < 2.363 -

Synopsis

An application running on a remote web server host is affected by a vulnerability

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.361.1 or Jenkins weekly prior to 2.363. It is, therefore, affected by a vulnerability:

- In Eclipse Jetty HTTP/2 server implementation, when encountering an invalid HTTP/2 request, the error handling has a bug that can wind up not properly cleaning up the active connections and associated resources. This can lead to a Denial of Service scenario where there are no enough resources left to process good requests. (CVE-2022-2048)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2022-09-09

Solution

Upgrade Jenkins weekly to version 2.363 or later, or Jenkins LTS to version 2.361.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:C)

References

CVE	CVE-2022-2048

Plugin Information

Published: 2022/09/09, Modified: 2024/06/04

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.361.1
```

177395 - Jenkins LTS < 2.401.1 / Jenkins weekly < 2.400 XSRF -

Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.401.1 or Jenkins weekly prior to 2.400. It is, therefore, affected by the following vulnerability:

- In Jenkins 2.399 and earlier, LTS 2.387.3 and earlier, POST requests are sent in order to load the list of context actions. If part of the URL includes insufficiently escaped user-provided values, a victim may be tricked into sending a POST request to an unexpected endpoint by opening a context menu. (CVE-2023-35141)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2023-06-14

Solution

Upgrade Jenkins weekly to version 2.400 or later, or Jenkins LTS to version 2.401.1 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.0 (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-35141
XREF	JENKINS:2023-06-14
XREF	IAVA:2023-A-0309-S

Plugin Information

Published: 2023/06/16, Modified: 2024/06/04

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.401.1
```

181682 - Jenkins LTS < 2.414.2 / Jenkins weekly < 2.424 Multiple Vulnerabilities -

Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.414.2 or Jenkins weekly prior to 2.424. It is, therefore, affected by multiple vulnerabilities:

- Jenkins 2.50 through 2.423 (both inclusive), LTS 2.60.1 through 2.414.1 (both inclusive) does not exclude sensitive build variables (e.g., password parameter values) from the search in the build history widget, allowing attackers with Item/Read permission to obtain values of sensitive variables used in builds by iteratively testing different characters until the correct sequence is discovered. (CVE-2023-43494)

- In Jenkins 2.423 and earlier, LTS 2.414.1 and earlier, processing file uploads using the Stapler web framework creates temporary files in the default system temporary directory with the default permissions for newly created files, potentially allowing attackers with access to the Jenkins controller file system to read and write the files before they are used. (CVE-2023-43497)

- In Jenkins 2.423 and earlier, LTS 2.414.1 and earlier, processing file uploads using MultipartFormDataParser creates temporary files in the default system temporary directory with the default permissions for newly created files, potentially allowing attackers with access to the Jenkins controller file system to read and write the files before they are used. (CVE-2023-43498)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2023-09-20

Solution

Upgrade Jenkins weekly to version 2.424 or later, or Jenkins LTS to version 2.414.2 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-43494
CVE	CVE-2023-43495
CVE	CVE-2023-43496
CVE	CVE-2023-43497
CVE	CVE-2023-43498
XREF	JENKINS:2023-09-20
XREF	IAVA:2023-A-0502-S

Plugin Information

Published: 2023/09/20, Modified: 2024/06/04

Plugin Output

tcp/8081/www

```
Product : Jenkins Open Source LTS
URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
Installed version : 2.150.2
Fixed version : 2.414.2
```

183316 - Jenkins LTS < 2.414.3 / Jenkins weekly < 2.428 Multiple Vulnerabilities -

Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.414.3 or Jenkins weekly prior to 2.428. It is, therefore, affected by multiple vulnerabilities:

- Eclipse Jetty provides a web server and servlet container. In versions 11.0.0 through 11.0.15, 10.0.0 through 10.0.15, and 9.0.0 through 9.4.52, an integer overflow in `MetaDataBuilder.checkSize` allows for HTTP/2 HPACK header values to exceed their size limit. `MetaDataBuilder.java` determines if a header name or value exceeds the size limit, and throws an exception if the limit is exceeded. However, when length is very large and huffman is true, the multiplication by 4 in line 295 will overflow, and length will become negative. `(_size+length)` will now be negative, and the check on line 296 will not be triggered.
Furthermore, `MetaDataBuilder.checkSize` allows for user-entered HPACK header value sizes to be negative, potentially leading to a very large buffer allocation later on when the user-entered size is multiplied by 2. This means that if a user provides a negative length value (or, more precisely, a length value which, when multiplied by the 4/3 fudge factor, is negative), and this length value is a very large positive number when multiplied by 2, then the user can cause a very large buffer to be allocated on the server.
Users of HTTP/2 can be impacted by a remote denial of service attack. The issue has been fixed in versions 11.0.16, 10.0.16, and 9.4.53. There are no known workarounds. (CVE-2023-36478)

- The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023. (CVE-2023-44487)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2023-10-18

Solution

Upgrade Jenkins weekly to version 2.428 or later, or Jenkins LTS to version 2.414.3 or later.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

6.4 (CVSS2#E:F/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-36478
CVE	CVE-2023-44487
XREF	CISA-KNOWN-EXPLOITED:2023/10/31
XREF	JENKINS:2023-10-18

XREF	CEA-ID:CEA-2024-0004
XREF	IAVB:2023-B-0083-S

Plugin Information

Published: 2023/10/18, Modified: 2024/06/04

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.414.3
```

192307 - Jenkins LTS < 2.440.2 / Jenkins weekly < 2.444 -

Synopsis

An application running on a remote web server host is affected by a vulnerability

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.440.2 or Jenkins weekly prior to 2.444. It is, therefore, affected by a vulnerability:

- Jetty is a Java based web server and servlet engine. An HTTP/2 SSL connection that is established and TCP congested will be leaked when it times out. An attacker can cause many connections to end up in this state, and the server may run out of file descriptors, eventually causing the server to stop accepting new connections from valid clients. The vulnerability is patched in 9.4.54, 10.0.20, 11.0.20, and 12.0.6.
(CVE-2024-22201)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2024-03-20

Solution

Upgrade Jenkins weekly to version 2.444 or later, or Jenkins LTS to version 2.440.2 or later.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2024-22201
XREF	JENKINS:2024-03-20

Plugin Information

Published: 2024/03/20, Modified: 2024/06/04

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.440.2
```

205143 - Jenkins LTS < 2.452.4 / Jenkins weekly < 2.471 Multiple Vulnerabilities -

Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.452.4 or Jenkins weekly prior to 2.471. It is, therefore, affected by multiple vulnerabilities:

- Jenkins 2.470 and earlier, LTS 2.452.3 and earlier allows agent processes to read arbitrary files from the Jenkins controller file system by using the `ClassLoaderProxy#fetchJar` method in the Remoting library.
(CVE-2024-43044)

- Jenkins 2.470 and earlier, LTS 2.452.3 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to access other users' My Views.
(CVE-2024-43045)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2024-08-07

Solution

Upgrade Jenkins weekly to version 2.471 or later, or Jenkins LTS to version 2.452.4 or 2.462.1 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2024-43044
CVE	CVE-2024-43045
XREF	JENKINS:2024-08-07
XREF	IAVA:2024-A-0472-S

Plugin Information

Published: 2024/08/07, Modified: 2024/10/04

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.452.4 or 2.462.1
```

142960 - HSTS Missing From HTTPS Server (RFC 6797) -

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

Plugin Output

tcp/443/www

```
  HTTP/1.1 302 Found
  Date: Wed, 13 Nov 2024 15:59:01 GMT
  Server: Apache
  X-Frame-Options: SAMEORIGIN
  Location: https://13.52.135.157/
  Content-Length: 206
  Connection: close
  Content-Type: text/html; charset=iso-8859-1


  The remote HTTPS server does not send the HTTP
  "Strict-Transport-Security" header.
```

138887 - Jenkins (< 2.235.2 LTS / < 2.245 Weekly) Multiple Stored XSS (Jenkins Security Advisory 2020-07-15) -

Synopsis

A job scheduling and management system hosted on the remote web server is affected by multiple stored XSS vulnerabilities.

Description

The version of Jenkins running on the remote web server is prior to 2.245 or is a version of Jenkins LTS prior to 2.235.2. It is, therefore, affected by multiple stored cross-site scripting (XSS) vulnerabilities in various components including its build time trend page, build cause page, tooltips & build console page. This is due to improper validation of user-supplied input before returning it to users. An authenticated, remote attacker can exploit this, by convincing a user to click a specially crafted URL, to execute arbitrary script code in a user's browser session.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?1846d83d

Solution

Upgrade Jenkins weekly to version 2.245 or later. Upgrade Jenkins LTS to version 2.235.2 or later.

Risk Factor

Low

CVSS v3.0 Base Score

5.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

3.5 (CVSS2#AV:N/AC:M/Au:S/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

2.6 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2020-2220
CVE	CVE-2020-2221
CVE	CVE-2020-2222
CVE	CVE-2020-2223
XREF	IAVA:2020-A-0337-S

Plugin Information

Published: 2020/07/24, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.235.2 LTS / 2.245
```

130099 - Jenkins < 2.176.4 LTS / 2.197 Multiple Vulnerabilities -

Synopsis

A job scheduling and management system hosted on the remote web server is affected by multiple vulnerabilities.

Description

The version of Jenkins running on the remote web server is prior to 2.197 or is a version of Jenkins LTS prior to 2.176.4. It is, therefore, affected by multiple vulnerabilities:

- An information disclosure vulnerability exists in the /whoAmI/ URL due to the exposed 'Cookie' HTTP Header. An authenticated, remote attacker can exploit this, via a separate Cross-site scripting (XSS) vulnerability, to disclose potentially sensitive information. (CVE-2019-10405)

- A stored Cross-site scripting (XSS) vulnerability exists in the f:formbox form control due to the form control interpreting its item labels as HTML. An authenticated, remote attacker with permission to control the contents of f:formbox form controls can exploit this to execute arbitrary script code in a user's browser session. (CVE-2019-10402)

- A stored Cross-site scripting (XSS) vulnerability exists in the tooltip for SCM tag actions due to the application not escaping characters in the SCM tag name. An authenticated, remote attacker with permission to control SCM tag names can exploit this to execute arbitrary code in a user's browser session. (CVE-2019-10403)

The version of Jenkins running on the remote web server is also affected by other Cross-site scripting (XSS) vulnerabilities. (CVE-2019-10401, CVE-2019-10404, CVE-2019-10406)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2019-09-25/

Solution

Upgrade Jenkins to version 2.197 or later, Jenkins LTS to version 2.176.4 or later.

Risk Factor

Low

CVSS v3.0 Base Score

5.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

3.5 (CVSS2#AV:N/AC:M/Au:S/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

2.6 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2019-10401
CVE	CVE-2019-10402
CVE	CVE-2019-10403
CVE	CVE-2019-10404
CVE	CVE-2019-10405
CVE	CVE-2019-10406

Plugin Information

Published: 2019/10/21, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
Product : Jenkins Open Source LTS
URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
Installed version : 2.150.2
Fixed version : 2.176.4 LTS / 2.197
```

133527 - Jenkins < 2.204.2 LTS / 2.219 Multiple Vulnerabilities -

Synopsis

A job scheduling and management system hosted on the remote web server is affected by multiple vulnerabilities.

Description

The version of Jenkins running on the remote web server is prior to 2.219 or is a version of Jenkins LTS prior to 2.204.2. It is, therefore, affected by multiple vulnerabilities:

- An UDP amplification reflection attack can be used in a DDoS attack on a Jenkins master. Within the same network, spoofed UDP packets could also be sent to make two Jenkins masters go into an infinite loop of replies to one another, thus causing a denial of service.
(CVE-2020-2100)

- A non-constant time comparison of inbound TCP agent connection secret is used when an inbound TCP agent connection is initiated. This allows attackers to use statistical methods to obtain the connection secret.
(CVE-2020-2101)

- A non-constant time HMAC comparison is used when checking whether two HMACs are equal. This could potentially allow attackers to use statistical methods to obtain a valid HMAC for an attacker-controlled input value. (CVE-2020-2102)

- User metadata on the /whoAmI page includes the HTTP session ID which allows attackers able to exploit a cross-site scripting vulnerability to obtain the HTTP session ID value. (CVE-2020-2103)

- A lack of appropriate permissions allows anyone with Overall/Read permissions to access the JVM memory usage chart for the Jenkins master.
(CVE-2020-2104)

- The Jenkins REST APIs allows an attacker to perform a clickjacking attack by routing them to a specially crafted web page, and can expose the content of the REST API endpoint. (CVE-2020-2105)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2020-01-29/

Solution

Upgrade Jenkins to version 2.219 or later, Jenkins LTS to version 2.204.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

5.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2020-2100
CVE	CVE-2020-2101
CVE	CVE-2020-2102
CVE	CVE-2020-2103
CVE	CVE-2020-2104
CVE	CVE-2020-2105
CVE	CVE-2020-2106

Plugin Information

Published: 2020/02/06, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.204.2 LTS / 2.219
```

139726 - Jenkins < 2.235.4 LTS / 2.252 Multiple Cross-Site Scripting (XSS) Vulnerabilities -

Synopsis

A job scheduling and management system hosted on the remote web server is affected by multiple cross-site scripting vulnerabilities.

Description

The version of Jenkins running on the remote web server is prior to 2.252 or is a version of Jenkins LTS prior to 2.235.4. It is, therefore, affected by multiple cross-site scripting vulnerabilities due to improper validation of user-supplied input before returning it to users. An authenticated, remote attacker can exploit this to execute arbitrary script code in a user's browser session.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2020-08-12/

Solution

Upgrade Jenkins to version 2.252 or later, Jenkins LTS to version 2.235.4 or later.

Risk Factor

Low

CVSS v3.0 Base Score

5.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.9 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

3.5 (CVSS2#AV:N/AC:M/Au:S/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

2.7 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2020-2229
CVE	CVE-2020-2230
CVE	CVE-2020-2231
XREF	IAVA:2020-A-0380-S

Plugin Information

Published: 2020/08/20, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
Product : Jenkins Open Source LTS
URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
Installed version : 2.150.2
Fixed version : 2.235.4 LTS / 2.252
```

145533 - Jenkins < 2.263.3 LTS / 2.276 TOCTOU -

Synopsis

A job scheduling and management system hosted on the remote web server is affected by a time-of-check to time-of-use race condition.

Description

The version of Jenkins running on the remote web server is prior to 2.276 weekly or 2.263.3 LTS. It is, therefore, affected by a time-of-check to time-of-use (TOCTOU) race condition that allows reading arbitrary files using the file browser for workspaces and archived artifacts.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.jenkins.io/security/advisory/2021-01-26/

Solution

Upgrade Jenkins to version 2.276 or later, Jenkins LTS to version 2.263.3 or later.

Risk Factor

Low

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

3.5 (CVSS2#AV:N/AC:M/Au:S/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

2.6 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-21615
XREF	IAVA:2021-A-0047-S

Plugin Information

Published: 2021/01/28, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
Product : Jenkins Open Source LTS
URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
Installed version : 2.150.2
Fixed version : 2.263.3 LTS / 2.276
```

148418 - Jenkins LTS < 2.277.2 / Jenkins weekly < 2.287 Multiple Vulnerabilities -

Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.277.2 or Jenkins weekly prior to 2.287. It is, therefore, affected by multiple vulnerabilities:

- Jenkins 2.286 and earlier, LTS 2.277.1 and earlier does not validate the type of object created after loading the data submitted to the `config.xml` REST API endpoint of a node, allowing attackers with Computer/Configure permission to replace a node with one of a different type. (CVE-2021-21639)

- Jenkins 2.286 and earlier, LTS 2.277.1 and earlier does not properly check that a newly created view has an allowed name, allowing attackers with View/Create permission to create views with invalid or already- used names. (CVE-2021-21640)

- A cross-site request forgery (CSRF) vulnerability in Jenkins promoted builds Plugin 3.9 and earlier allows attackers to to promote builds. (CVE-2021-21641)
- Improper Certificate Validation vulnerability in Micro Focus Application Automation Tools Plugin - Jenkins plugin. The vulnerability affects version 6.7 and earlier versions. The vulnerability could allow unconditionally disabling of SSL/TLS certificates. (CVE-2021-22511)
- Cross-Site Request Forgery (CSRF) vulnerability in Micro Focus Application Automation Tools Plugin - Jenkins plugin. The vulnerability affects version 6.7 and earlier versions. The vulnerability could allow form validation without permission checks. (CVE-2021-22512)
- Missing Authorization vulnerability in Micro Focus Application Automation Tools Plugin - Jenkins plugin. The vulnerability affects version 6.7 and earlier versions. The vulnerability could allow access without permission checks. (CVE-2021-22513)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2021-04-07

Solution

Upgrade Jenkins weekly to version 2.287 or later or Jenkins LTS to version 2.277.2 or later

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2021-21639
CVE	CVE-2021-21640
CVE	CVE-2021-21641
CVE	CVE-2021-22510
CVE	CVE-2021-22511
CVE	CVE-2021-22512
CVE	CVE-2021-22513

Plugin Information

Published: 2021/04/09, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
Product : Jenkins Open Source LTS
URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
Installed version : 2.150.2
Fixed version : 2.277.2
```

154055 - Jenkins LTS < 2.303.2 / Jenkins weekly < 2.315 Multiple Vulnerabilities -

Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.303.2 or Jenkins weekly prior to 2.315. It is, therefore, affected by multiple vulnerabilities:

- Jenkins 2.314 and earlier, LTS 2.303.1 and earlier accepts names of jobs and other entities with a trailing dot character, potentially replacing the configuration and data of other entities on Windows.
(CVE-2021-21682)

- org.apache.http.conn.ssl.AbstractVerifier in Apache HttpComponents HttpClient before 4.3.5 and HttpAsyncClient before 4.0.2 does not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the- middle attackers to spoof SSL servers via a CN= string in a field in the distinguished name (DN) of a certificate, as demonstrated by the foo,CN=www.apache.org string in the O field. (CVE-2014-3577)

- The file browser in Jenkins 2.314 and earlier, LTS 2.303.1 and earlier may interpret some paths to files as absolute on Windows, resulting in a path traversal vulnerability allowing attackers with Overall/Read permission (Windows controller) or Job/Workspace permission (Windows agents) to obtain the contents of arbitrary files. (CVE-2021-21683)

- Jenkins Git Plugin 4.8.2 and earlier does not escape the Git SHA-1 checksum parameters provided to commit notifications when displaying them in a build cause, resulting in a stored cross-site scripting (XSS) vulnerability. (CVE-2021-21684)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2021-10-06

Solution

Upgrade Jenkins weekly to version 2.315 or later or Jenkins LTS to version 2.303.2 or later

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.5 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2014-3577
CVE	CVE-2021-21682
CVE	CVE-2021-21683

CVE	CVE-2021-21684
XREF	IAVA:2021-A-0460-S

Plugin Information

Published: 2021/10/13, Modified: 2024/06/05

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.303.2
```

178903 - Jenkins LTS < 2.401.3 / Jenkins weekly < 2.416 Multiple Vulnerabilities -

Synopsis

An application running on a remote web server host is affected by a vulnerability

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.401.3 or Jenkins weekly prior to 2.416. It is, therefore, affected by multiple vulnerabilities:

- Jenkins 2.415 and earlier, LTS 2.401.2 and earlier does not sanitize or properly encode URLs in build logs when transforming them into hyperlinks, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control build log contents. (CVE-2023-39151)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2023-07-26

Solution

Upgrade Jenkins weekly to version 2.416 or later, or Jenkins LTS to version 2.401.3 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

5.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-39151
XREF	JENKINS:2023-07-26
XREF	IAVA:2023-A-0384-S

Plugin Information

Published: 2023/07/26, Modified: 2024/06/04

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.401.3
```

193426 - Jenkins LTS < 2.440.3 / Jenkins weekly < 2.452 -

Synopsis

An application running on a remote web server host is affected by a vulnerability

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.440.3 or Jenkins weekly prior to 2.452. It is, therefore, affected by a vulnerability:

- The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. (CVE-2023-48795)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2024-04-17

Solution

Upgrade Jenkins weekly to version 2.452 or later, or Jenkins LTS to version 2.440.3 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

5.4 (CVSS2#AV:N/AC:H/Au:N/C:N/I:C/A:N)

CVSS v2.0 Temporal Score

4.2 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2023-48795
XREF	JENKINS:2024-04-17

Plugin Information

Published: 2024/04/17, Modified: 2024/06/04

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.440.3
```

208098 - Jenkins LTS < 2.462.3 / Jenkins weekly < 2.479 Multiple Vulnerabilities -

Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities

Description

According to its its self-reported version number, the version of Jenkins running on the remote web server is Jenkins LTS prior to 2.462.3 or Jenkins weekly prior to 2.479. It is, therefore, affected by multiple vulnerabilities:

- Jenkins 2.478 and earlier, LTS 2.462.2 and earlier does not redact multi-line secret values in error messages generated for form submissions involving the `secretTextarea` form field. (CVE-2024-47803)

- If an attempt is made to create an item of a type prohibited by `ACL#hasCreatePermission2` or `TopLevelItemDescriptor#isApplicableIn(ItemGroup)` through the Jenkins CLI or the REST API and either of these checks fail, Jenkins 2.478 and earlier, LTS 2.462.2 and earlier creates the item in memory, only deleting it from disk, allowing attackers with Item/Configure permission to save the item to persist it, effectively bypassing the item creation restriction. (CVE-2024-47804)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://jenkins.io/security/advisory/2024-10-02

Solution

Upgrade Jenkins weekly to version 2.479 or later, or Jenkins LTS to version 2.462.3 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

4.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.8 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2024-47803
CVE	CVE-2024-47804
XREF	JENKINS:2024-10-02
XREF	IAVA:2024-A-0606

Plugin Information

Published: 2024/10/03, Modified: 2024/10/04

Plugin Output

tcp/8081/www

```
  Product : Jenkins Open Source LTS
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Installed version : 2.150.2
  Fixed version : 2.462.3
```

48204 - Apache HTTP Server Version -

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com/
  Version : unknown
  Source : Server: Apache
  backported : 0
```

48204 - Apache HTTP Server Version -

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/443/www

```
URL : https://ec2-13-52-135-157.us-west-1.compute.amazonaws.com/
Version : unknown
Source : Server: Apache
backported : 0
```

194915 - Eclipse Jetty Web Server Detection -

Synopsis

The Eclipse Jetty web server was detected on the remote host.

Description

The Eclipse Jetty web server was detected on the remote host.

See Also

https://eclipse.dev/jetty/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/05/02, Modified: 2024/10/10

Plugin Output

tcp/0

```
URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
Version : 9.4
Source : Server: Jetty(9.4.z-SNAPSHOT)
```

84502 - HSTS Missing From HTTPS Server -

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

Plugin Output

tcp/443/www

```
  HTTP/1.1 302 Found
  Date: Wed, 13 Nov 2024 15:59:01 GMT
  Server: Apache
  X-Frame-Options: SAMEORIGIN
  Location: https://13.52.135.157/
  Content-Length: 206
  Connection: close
  Content-Type: text/html; charset=iso-8859-1


  The remote HTTPS server does not send the HTTP
  "Strict-Transport-Security" header.
```

69826 - HTTP Cookie 'secure' Property Transport Mismatch -

Synopsis

The remote web server sent out a cookie with a secure property that does not match the transport on which it was sent.

Description

The remote web server sends out cookies to clients with a 'secure'
property that does not match the transport, HTTP or HTTPS, over which they were received. This may occur in two forms :

1. The cookie is sent over HTTP, but has the 'secure'
property set, indicating that it should only be sent over a secure, encrypted transport such as HTTPS.
This should not happen.

2. The cookie is sent over HTTPS, but has no 'secure'
property set, indicating that it may be sent over both HTTP and HTTPS transports. This is common, but care should be taken to ensure that the 'secure' property not being set is deliberate.

See Also

https://tools.ietf.org/html/rfc6265

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/09/10, Modified: 2021/12/20

Plugin Output

tcp/443/www

```
The following cookie does not have the 'secure' property enabled, despite being served over HTTPS :

Domain :
Path : /
Name : JSESSIONID.ce8274c2
Value : node0wlljyx221yot13fq1wbh24nih28052.node0
Secure : false
HttpOnly : true
```

43111 - HTTP Methods Allowed (per directory) -

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a
http://www.nessus.org/u?b019cbdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/

- Invalid/unknown HTTP methods are allowed on :

/
```

43111 - HTTP Methods Allowed (per directory) -

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a
http://www.nessus.org/u?b019cbdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/

- Invalid/unknown HTTP methods are allowed on :

/
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/443/www

```
The remote web server type is :

Apache
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8081/www

```
The remote web server type is :

Jetty(9.4.z-SNAPSHOT)
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

```

Response Code : HTTP/1.1 302 Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Wed, 13 Nov 2024 16:27:29 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Location: http://13.52.135.157/
Content-Length: 205
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="http://13.52.135.157/">here</a>.</p>
</body></html>
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/443/www

```

  Response Code : HTTP/1.1 302 Found

  Protocol version : HTTP/1.1
  HTTP/2 TLS Support: No
  HTTP/2 Cleartext Support: No
  SSL : yes
  Keep-Alive : yes
  Options allowed : (Not implemented)
  Headers :

  Date: Wed, 13 Nov 2024 16:27:36 GMT
  Server: Apache
  X-Frame-Options: SAMEORIGIN
  Location: https://13.52.135.157/
  Content-Length: 206
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1

  Response Body :

  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
  <html><head>
  <title>302 Found</title>
  </head><body>
  <h1>Found</h1>
  <p>The document has moved <a href="https://13.52.135.157/">here</a>.</p>
  </body></html>
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8081/www

```
Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Connection: close
Date: Wed, 13 Nov 2024 16:27:32 GMT
X-Content-Type-Options: nosniff
Content-Type: text/html;charset=utf-8
X-Hudson: 1.395
X-Jenkins: 2.150.2
X-Jenkins-Session: cb153f45
X-You-Are-Authenticated-As: anonymous
X-You-Are-In-Group-Disabled: JENKINS-39402: use -Dhudson.security.AccessDeniedException2.REPORT_GROUP_HEADERS=true or use
/whoAmI to diagnose
X-Required-Permission: hudson.model.Hudson.Read
X-Permission-Implied-By: hudson.security.Permission.GenericRead
X-Permission-Implied-By: hudson.model.Hudson.Administer
Content-Length: 793
Server: Jetty(9.4.z-SNAPSHOT)

Response Body :

<html><head><meta http-equiv='refresh' content='1;url=/login?from=%2F'/><script>window.location.replace('/login?
from=%2F');</script></head><body style='background-color:white; color:white;'>


Authentication required
<!--
You are authenticated as: anonymous
Groups that you are in:

Permission you need to have (but didn't): hudson.model.Hudson.Read
... which is implied by: hudson.security.Permission.GenericRead
... which is implied by: hudson.model.Hudson.Administer
-->

</body></html>
```

91634 - HyperText Transfer Protocol (HTTP) Redirect Information -

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Risk Factor

None

Plugin Information

Published: 2016/06/16, Modified: 2017/10/12

Plugin Output

tcp/80/www

```
  Request : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com/
  HTTP response : HTTP/1.1 302 Found
  Redirect to : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com/
  Redirect type : 30x redirect

  Request : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com/
  HTTP response : HTTP/1.1 302 Found
  Redirect to : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com/
  Redirect type : 30x redirect

  Final page : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com/
  HTTP response : HTTP/1.1 302 Found



  Note that Nessus did not receive a 200 OK response from the
  last examined redirect.
```

91634 - HyperText Transfer Protocol (HTTP) Redirect Information -

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Risk Factor

None

Plugin Information

Published: 2016/06/16, Modified: 2017/10/12

Plugin Output

tcp/443/www

```
  Request : https://ec2-13-52-135-157.us-west-1.compute.amazonaws.com/
  HTTP response : HTTP/1.1 302 Found
  Redirect to : https://13.52.135.157/
  Redirect type : 30x redirect

  Request : https://ec2-13-52-135-157.us-west-1.compute.amazonaws.com/
  HTTP response : HTTP/1.1 302 Found
  Redirect to : https://13.52.135.157/
  Redirect type : 30x redirect

  Final page : https://ec2-13-52-135-157.us-west-1.compute.amazonaws.com/
  HTTP response : HTTP/1.1 302 Found



  Note that Nessus did not receive a 200 OK response from the
  last examined redirect.
```

65054 - Jenkins Detection -

Synopsis

The remote web server hosts a job scheduling / management system.

Description

The remote web server hosts Jenkins, a job scheduling / management system and a drop-in replacement for Hudson.

See Also

https://jenkins.io/index.html
https://www.cloudbees.com/jenkins/about

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0638

Plugin Information

Published: 2013/03/06, Modified: 2024/10/03

Plugin Output

tcp/8081/www

```
  URL : http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com:8081/
  Version : 2.150.2
  Edition : Open Source LTS
  Hudson Version : 1.395
  LTS : 1
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/22/ssh

```
  Port 22/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/80/www

```
  Port 80/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/443/www

```
  Port 443/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/8081/www

```
Port 8081/tcp was found to be open
```

19506 - Nessus Scan Information -

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/10/04

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202411131243
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : raspberrypios_armhf
Scan type : Normal
Scan name : shopcart
Scan policy used : Web Application Tests
Scanner IP : 192.168.0.113
```

```
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 192.762 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests - Test mode : single
Web app tests - Try all HTTP methods : no
Web app tests - Maximum run time : 5 minutes.
Web app tests - Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/11/13 18:56 +03
Scan duration : 3442 sec
Scan for malware : no
```

66334 - Patch Report -

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/11/12

Plugin Output

tcp/0

```
. You need to take the following action :

[ Jenkins LTS < 2.462.3 / Jenkins weekly < 2.479 Multiple Vulnerabilities (208098) ]

+ Action to take : Upgrade Jenkins weekly to version 2.479 or later, or Jenkins LTS to version 2.462.3 or later.

+Impact : Taking this action will resolve 168 different vulnerabilities (CVEs).
```

85602 - Web Application Cookies Not Marked Secure -

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'
cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

https://www.owasp.org/index.php/SecureFlag

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:522
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/80/www

```
The following cookie does not set the secure cookie flag :

Name : JSESSIONID.ce8274c2
Path : /
Value : node0wlljyx221yot13fq1wbh24nih28052.node0
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :
```

85602 - Web Application Cookies Not Marked Secure -

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'
cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

https://www.owasp.org/index.php/SecureFlag

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:522
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/443/www

```
  The following cookie does not set the secure cookie flag :

  Name : JSESSIONID.ce8274c2
  Path : /
  Value : node0wlljyx221yot13fq1wbh24nih28052.node0
  Domain :
  Version : 1
  Expires :
  Comment :
  Secure : 0
  Httponly : 1
  Port :
```

85602 - Web Application Cookies Not Marked Secure -

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'
cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

https://www.owasp.org/index.php/SecureFlag

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:522
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/8081/www

```
The following cookie does not set the secure cookie flag :

Name : JSESSIONID.ce8274c2
Path : /
Value : node0wlljyx221yot13fq1wbh24nih28052.node0
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :
```

10386 - Web Server No 404 Error Code Check -

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/80/www

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 302
rather than 404. The requested URL was :

http://ec2-13-52-135-157.us-west-1.compute.amazonaws.com/5J9bUgMFsweR.html
```

10386 - Web Server No 404 Error Code Check -

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/443/www

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 302
rather than 404. The requested URL was :

https://ec2-13-52-135-157.us-west-1.compute.amazonaws.com/5J9bUgMFsweR.html
```

10302 - Web Server robots.txt Information Disclosure -

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/8081/www

```
Contents of robots.txt :

# we don't want robots to click "build" links
User-agent: *
Disallow: /
```