



CVE-2021-25646

Published on: 01/29/2021 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2021-25646

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

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

Apache Druid includes the ability to execute user-provided JavaScript code embedded in various types of requests. This functionality is intended for use in high-trust environments, and is disabled by default. However, in Druid 0.20.0 and earlier, it is possible for an authenticated user to send a specially-crafted request that forces Druid to run user-

provided JavaScript code for that request, regardless of server configuration. This can be leveraged to execute code on the target machine with the privileges of the Druid server process.

CVE-2021-25646 has been assigned by security@apache.org to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Apache Software Foundation - Apache Druid** version **<= 0.20.0**

Vulnerability Patch/Work Around

Users should upgrade to Druid 0.20.1. Whenever possible, network access to cluster machines should be restricted to trusted hosts only.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE
CVE References		
Description	Tags	Link
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [druid-commits] 20210204 [GitHub] [druid] jihoonson merged pull request #10854: [Backg
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [druid-commits] 20210204 [GitHub] [druid] jihoonson commented on pull request #10818
Pony Mail!	lists.apache.org text/html	 MLIST [druid-dev] 20210331 Regarding the 0.21.0 release
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [druid-dev] 20210129 Re: [druid-user] Re: CVE-2021-25646: Authenticated users can ov their requests which allows them to execute arbitrary code.
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MISC lists.apache.org/thread.html/rfda8a3aa6ac06a80c5cbfdeae0fc85f88a5984e32ea05e6dda46f866%4
Pony Mail!	lists.apache.org text/html	 MLIST [druid-commits] 20210205 [GitHub] [druid] jihoonson opened a new pull request #10854: 25646
oss-security - CVE-2021-25646: Authenticated users can override system configurations in their requests which allows them to execute arbitrary code.	Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20210129 CVE-2021-25646: Authenticated users can override system con which allows them to execute arbitrary code.
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [druid-commits] 20210204 [GitHub] [druid] jihoonson merged pull request #10818: Fix CV
Pony Mail!	lists.apache.org text/html	 MLIST [druid-commits] 20210205 [GitHub] [druid] jihoonson merged pull request #10854: [Backg
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [druid-commits] 20210204 [GitHub] [druid] jihoonson opened a new pull request #10854: 25646
Pony Mail!	lists.apache.org text/html	 MLIST [druid-commits] 20210205 [GitHub] [druid] jihoonson commented on pull request #10818

Pony Mail!

Mailing List

Vendor Advisory

lists.apache.org

text/html

🔥

MLIST [druid-dev] 20210129 Re: CVE-2021-25646: Authenticated users can override system co which allows them to execute arbitrary code.

Apache Druid
0.20.0
Remote
Command
Execution ≈
Packet Storm

packetstormsecurity.com

text/html

📄

MISC packetstormsecurity.com/files/162345/Apache-Druid-0.20.0-Remote-Command-Execution

Pony Mail!

lists.apache.org

text/html

🔥

MLIST [druid-commits] 20210205 [GitHub] [druid] jihoonson merged pull request #10818: Fix CV

Pony Mail!

Mailing List

Patch

Vendor Advisory

lists.apache.org

text/html

🔥

MLIST [druid-commits] 20210204 [druid] branch 0.21.0 updated: Fix CVE-2021-25646 (#10818)

Pony Mail!

Mailing List

Vendor Advisory

lists.apache.org

text/html

🔥

MLIST [announce] 20210129 Subject: [CVE-2021-25646] Apache Druid remote code execution

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.



Related QID Numbers

982234 Java (maven) Security Update for org.apache.druid:druid (GHSA-wrqf-rrrw-w3mg)

Exploit/POC from Github

Alibaba-Nacos-Unauthorized/ApacheDruid-RCE_CVE-2021-25646/MS-Exchange-SSRF-CVE-2021-26885/Oracle-WebLogic-CVE-2021-21...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Druid	All	All	All	All
cpe:2.3:a:apache:druid:*:*:*:*:*:						

Discovery Credit

This issue was discovered by Litch1 from the Security Team of Alibaba Cloud.

Social Mentions

Source	Title	Posted (UTC)
🇺🇸 GitHub	Alibaba-Nacos-Unauthorized/ApacheDruid-RCE_CVE-2021-25646/MS-Exchange-SSRF-CVE-2021-26885/Oracle-WebLogic-CVE-2021-21...	2021-02-01

🔒 @LinInfoSec	Apache - CVE-2021-25646: openwall.com/lists/oss-secu...	2021-03-31 23:30:55
🔒 @axcheron	CVE-2021-25646: Getting Code Execution on Apache Druid zerodayinitiative.com/blog/2021/3/25...	2021-04-01 04:28:00
🔒 @EsGeeks	Informe CVE-2021-25646 ? zerodayinitiative.com/blog/2021/3/25...	2021-04-01 17:58:57
🔒 @balcazarf	CVE-2021-25646 Druid Code Execution juni.pr/3sQqG8J https://t.co/K4uk39oxQt	2021-04-04 17:04:50
🔒 @Nick_nick310	githubを確認したり、ロジックを調べるのは難しいです。練習が必要ですね。Apache Druid 「CVE-2021-25646」の再現と修正点の確認 - Nickブログ nicksecuritylog.com/entry/2021/04/...	2021-04-11 22:30:06
🔒 @PentesterLab	Articles worth reading discovered last week: ? thezdi.com/blog/2021/3/25... ? robertchen.cc/blog/2021/04/0... ?... twitter.com/i/web/status/1...	2021-04-11 22:55:38
🔒 @Attackerkb_Bot	A new #attackerkb assesment on 'CVE-2021-25646' has been created by space-r7. Attacker Value: 4 Exploitability: 5 attackerkb.com/assessments/91...	2021-04-12 13:41:31
🔒 @JavaScript_b	Zero Day Initiative - CVE-2021-25646: Getting Code Execution on Apa... (Zero Day Initiative) Apache Druid is a hig... twitter.com/i/web/status/1...	2021-04-13 17:50:56
🔒 @InfoSec_b	Zero Day Initiative - CVE-2021-25646: Getting Code Execution on Apa... (Zero Day Initiative) Apache Druid is a hig... twitter.com/i/web/status/1...	2021-04-13 17:50:56
🔒 @PJ47596176	Not a Mystical attack helicopter as I orriginally suspected - Apache Druid. @thezdi zerodayinitiative.com/blog/2021/3/25...	2021-05-12 20:22:18
🔒 @balcazarf	CVE-2021-25646 Druid Code Execution juni.pr/3ojiWKU https://t.co/vU6ewQi3Kc	2021-05-15 16:41:38
🔒 @subTee	Jackson shows up in the darndest places zerodayinitiative.com/blog/2021/3/25... "We deployed code in a fever, hotter than a pepper... twitter.com/i/web/status/1...	2021-09-10 03:10:09
🔒 @s3xcurlty	CVE-2021-25646 Apache Druid RCE POC gist.github.com/FanqXu/36c5e00... #InfoSec #CyberSecurity #Apache #RCE	2021-09-14 15:48:25
🔒 @ipssignatures	It's new to me that Astaro has a protection/signature/rule for the vulnerability CVE-2021-25646.... twitter.com/i/web/status/1...	2021-10-30 22:02:01
🔒 @ipssignatures	I know 4 other IPSs that have protections/signatures/rules for the vulnerability CVE-2021-25646. ipssignatures.appspot.com/?cve=CVE-2021-... #Shmt7b264yy3cs	2021-10-30 22:02:01
🔒 @OPOSEC	Getting Code Execution on Apache Druid (CVE-2021-25646). bit.ly/39VqsWI (+) #Security #373 (2021)	2023-01-18 08:00:02

← Previous ID

Next ID →

© CVE.report 2023 🔒 N |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/).

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