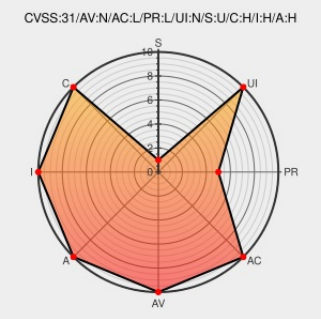
CVE-2022-36364

Published on: Not Yet Published

Last Modified on: 08/03/2022 07:36:00 PM UTC

CVE-2022-36364

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



Certain versions of Apache Calcite Avatica from Apache contain the following vulnerability:

Apache Calcite Avatica JDBC driver creates HTTP client instances based on class names provided via `httpclient_impl` connection property; however, the driver does not verify if the class implements the expected interface before instantiating it, which can lead to code execution loaded via arbitrary classes and in rare cases remote code execution. To exploit the vulnerability: 1) the attacker needs to have privileges to control JDBC connection parameters; 2) and there should be a vulnerable class (constructor with URL parameter and ability to execute code) in the classpath. From Apache Calcite Avatica 1.22.0 onwards, it will be verified that the class implements the expected interface before invoking its constructor.

CVE-2022-36364 has been assigned by security@apache.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache Calcite Avatica** version **< 1.22.0**

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

CVE References

Description	Tags	Link
oss-security - CVE-2022-36364: Apache Calcite Avatica JDBC driver `httpclient_impl` connection property can be used as an RCE vector	www.openwall.com text/html	MLIST [oss-security] 20220728 CVE-2022-36364: Apache Calcite Avatica JDBC driver `httpclient_impl` connection property can be used as an RCE vector
No Description Provided	lists.apache.org	MISC

text/html lists.apache.org/thread/5csdj8bv4h3hfgw27okm84jh1j2fyw0c

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

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Apache Calcite Avatica	All	All	All	All

cpe:2.3:a:apache:apache_calcite_avatica:*:*:*:*:*:*:*:*:

Discovery Credit

Apache Calcite Avatica would like to thank Peter M (https://twitter.com/h1pmnh) for reporting this issue

Social Mentions

Source	Title	Posted (UTC)
@ApacheAvatica	Announcing Avatica version 1.22.0! Fixes CVE-2022-36364 ("httpclient_impl connection property can be used as an RCE… twitter.com/i/web/status/1…	2022-07-28 01:02:23
@CVEreport	CVE-2022-36364 : #Apache Calcite Avatica JDBC driver creates HTTP client instances based on class names provided vi… twitter.com/i/web/status/1…	2022-07-28 08:37:50
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-36364 Apache Calcite Avatica JDBC driver creates HTTP client instances… twitter.com/i/web/status/1…	2022-07-28 09:55:59
@oss_security	CVE-2022-36364: Apache Calcite Avatica JDBC driver `httpclient_impl` connection property can be used as an RCE vect… twitter.com/i/web/status/1…	2022-07-28 10:28:03
@h1pmnh	Awarded CVE-2022-36364 (), RCE in JDBC driver, on Apache Calcite Avatica project. Thanks to… twitter.com/i/web/status/1…	2022-07-28 11:14:44
@0_exploit	CVE-2022-36364 dlvr.it/SVf4KH	2022-07-28 11:25:12
@Har_sia	CVE-2022-36364 har-sia.info/CVE-2022-36364… #HarsiaInfo	2022-07-28 23:02:17
@the_yellow_fall	CVE-2022-36364: Apache Calcite Avatica Remote Code Execution securityonline.info/cve-2022-36364… #opensource #infosec #security #pentesting	2022-07-29 02:45:43
@AcooEdi	CVE-2022-36364: Apache Calcite Avatica Remote Code Execution dlvr.it/SVhF4g via securityonline https://t.co/1GUYkbPXIY	2022-07-29 02:49:33
@Komodosec	#Vulnerability #CVE202236364 CVE-2022-36364: Apache Calcite Avatica Remote Code Execution securityonline.info/cve-2022-36364…	2022-07-29 03:30:33
@ipssignatures	I know no IPS that has a protection/signature/rule for the vulnerability CVE-2022-36364. The vuln was published 0 d… twitter.com/i/web/status/1…	2022-07-29 06:04:01
@ipssignatures	The vuln CVE-2022-36364 has a tweet created 0 days ago and retweeted 8 times. twitter.com/h1pmnh/status/… #Smrer7p3tgr3a4	2022-07-29 06:04:01

	twitter.com/h1pmnh/status/… #Shrer7p3tqr3a4	06:04:01
@ipssignatures	The vuln CVE-2022-36364 has a tweet created 0 days ago and retweeted 10 times. twitter.com/h1pmnh/status/… #pow1rtrtwwcve	2022-07-29 08:06:00
@netsecu	api.follow.it/track-rss-stor… CVE-2022-36364: Apache Calcite Avatica Remote Code Execution #cybersecurity	2022-07-29 09:30:05
@Dinosn	CVE-2022-36364: Apache Calcite Avatica Remote Code Execution securityonline.info/cve-2022-36364…	2022-07-29 12:21:19
@ColorTokensInc	Emerging Vulnerability Found CVE-2022-36364 - Apache Calcite Avatica JDBC driver creates HTTP client instances base… twitter.com/i/web/status/1…	2022-07-29 12:21:25
@moton	CVE-2022-36364: Apache Calcite Avatica Remote Code Execution - securityonline.info/cve-2022-36364…	2022-07-29 13:55:42
@beingsheerazali	CVE-2022-36364: Apache Calcite Avatica Remote Code Execution securityonline.info/cve-2022-36364… Dinosn	2022-07-29 14:55:24
@Har_sia	CVE-2022-36364 har-sia.info/CVE-2022-36364… #HarsiaInfo	2022-07-29 23:00:12
@ptracesecurity	CVE-2022-36364: Apache Calcite Avatica JDBC driver `httpclient_impl` connection property can be used as an RCE vect… twitter.com/i/web/status/1…	2022-07-30 19:02:29
/r/netcve	CVE-2022-36364	2022-07-28 09:38:49
/r/KomodoCyberConsulting	CVE-2022-36364: Apache Calcite Avatica Remote Code Execution	2022-07-29 03:30:32

← Previous ID

Next ID→

© CVE.report 2023 | |

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

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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