

RTA Integrated RPA

Scanner: Using Components with Known Vulnerabilities

Scan Time: 09/06/2021 10:03:24

Results:

[!] Scanned file: <https://www.etsy.com/paula/v3/polyfill.min.js?etsy-v=v2&flags=gated&ua-hash=e5d34a2af>

[-] No vulnerabilities found

[!] Scanned file: <https://www.etsy.com/ac/primary/js/en-US/core-libs.151c109354e88bbb86a1.js>

[+] Vulnerability found!

Severity: medium

CVE(s): ['CVE-2015-9251']

Summary: 3rd party CORS request may execute

Info:

<https://github.com/jquery/jquery/issues/2432>

<http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>

<https://nvd.nist.gov/vuln/detail/CVE-2015-9251>

<http://research.insecurelabs.org/jquery/test/>

Severity: medium

CVE(s): ['CVE-2015-9251']

Summary: parseHTML() executes scripts in event handlers

Info:

<https://bugs.jquery.com/ticket/11974>

<https://nvd.nist.gov/vuln/detail/CVE-2015-9251>

<http://research.insecurelabs.org/jquery/test/>

Severity: low

CVE(s): ['CVE-2019-11358']

Summary: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery

Info:

<https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/>

<https://nvd.nist.gov/vuln/detail/CVE-2019-11358>

<https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b>

[!] Scanned file: <https://www.etsy.com/ac/primary/js/en-US/base.250a91dbb296976dcef1.js>

[-] No vulnerabilities found

[!] Scanned file: <https://www.etsy.com/ac/primary/js/en-US/bootstrap/category-nav/v2/nav.70d52a7dcd469>

[-] No vulnerabilities found

[!] Scanned file: https://www.etsy.com/ac/primary/js/en-US/vesta_homepage/bootstrap.698e644ca554dae4

[-] No vulnerabilities found

[!] Scanned file: <https://www.etsy.com/ac/primary/js/en-US/neu-views/common/listing-card.c263c3837f7e1>

[-] No vulnerabilities found

[!] Server Version: Apache




National Vulnerability Database query result for [Apache]

Search Parameters:












- Results Type: Overview
- Keyword (text search): Apache
- Search Type: Search All




There are **2,197** matching records.
Displaying matches **1** through **20**.

1 2 3 4 5 6 7 8 9 10 > >>

Vuln ID 	Summary 	CVSS Severity 
CVE-2021-33190	<p>In Apache APISIX Dashboard version 2.6, we changed the default value of listen host to 0.0.0.0 in order to facilitate users to configure external network access. In the IP allowed list restriction, a risky function was used for the IP acquisition, which made it possible to bypass the network limit. At the same time, the default account and password are fixed. Ultimately these factors lead to the issue of security risks. This issue is fixed in APISIX Dashboard 2.6.1</p> <p>Published: June 08, 2021; 11:15:08 AM -0400</p>	<p>V3.x:(not available) V2.0:(not available)</p>
CVE-2021-30181	<p>Apache Dubbo prior to 2.6.9 and 2.7.9 supports Script routing which will enable a customer to route the request to the right server. These rules are used by the customers when making a request in order to find the right endpoint. When parsing these rules, Dubbo customers use ScriptEngine and run the rule provided by the script which by default may enable executing arbitrary code.</p> <p>Published: June 01, 2021; 10:15:09 AM -0400</p>	<p>V3.x:(not available) V2.0:(not available)</p>
CVE-2021-30180	<p>Apache Dubbo prior to 2.7.9 support Tag routing which will enable a customer to route the request to the right server. These rules are used by the customers when making a request in order to find the right endpoint. When parsing these YAML rules, Dubbo customers may enable calling arbitrary constructors.</p> <p>Published: June 01, 2021; 10:15:09 AM -0400</p>	<p>V3.x:(not available) V2.0:(not available)</p>
CVE-2021-30179	<p>Apache Dubbo prior to 2.6.9 and 2.7.9 by default supports generic calls to arbitrary methods exposed by provider interfaces. These invocations are handled by the GenericFilter which will find the service and method specified in the first arguments of the invocation and use the Java Reflection API to make the final call. The signature for the \$invoke or \$invokeAsync methods is Ljava/lang/String;[Ljava/lang/String;[Ljava/lang/Object; where the first argument is the</p>	<p>V3.x:(not available) V2.0:(not available)</p>

Exploit-DB query result for [Apache]





Exploit Database Advanced Search

Title

CVE

Type

Platform

Port

Content

Author

Tag

☐ Verified ☐ Has App ☐ No Metasploit

Show

Date	D	A	V	Title	Type	Platform	Author
2021-06-02				Apache Airflow 1.10.10 - 'Example Dag' Remote Code Execution	webapps	Multiple	Pepe Berba
2021-03-26				Apache Ghostcat CVE 2020-1938 - Paper	papers	Multiple	NAYAN DAS
2021-01-08				Apache Flink 1.11.0 - Unauthenticated Arbitrary File Read (Metasploit)	webapps	Java	SunCSR Team
2020-11-24				Apache OpenMeetings 5.0.0 - 'hostname' Denial of Service	webapps	Multiple	SunCSR
2020-11-17				Apache Struts 2.5.20 - Double OGNL evaluation	remote	Multiple	West Shepherd