

RTA Integrated RPA

Scanner: Using Components with Known Vulnerabilities

Scan Time: 16/06/2021 04:47:35

Results:

[!] Scanned file: <https://js.sentry-cdn.com/c46731518f4b4bd1b9c71cae6f3c5dd3.min.js>

[-] No vulnerabilities found

[!] 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/app-shell/globals/index.43e2fc4e40c3e7ec022e>

[-] No vulnerabilities found


[!] Scanned file: https://www.etsy.com/ac/primary/js/en-US/vesta_homepage/bootstrap.dabc94a07464823b

[-] No vulnerabilities found

[!] Scanned file: <https://www.etsy.com/ac/primary/js/en-US/neu-views/common/listing-card.ee4cbfc9bb4d0f>

[-] No vulnerabilities found

[!] Server Version: Apache



NVD MENU

[Information Technology Laboratory](#)


NATIONAL VULNERABILITY DATABASE

NVD

Timeout Error

Communication with back-end servers has timed out, this is usually a temporary error and the service will be available shortly. If this problem continues to occur, please send an email to nvd@nist.gov, along with a detailed description of the actions you attempted before this error was displayed.

Reference ID: NWVR-WEx




National Institute of
Standards and Technology
U.S. Department of Commerce


HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899
(301) 975-2000









Webmaster | [Contact Us](#) | [Our Other Offices](#)

Incident Response Assistance and Non-NVD Related
Technical Cyber Security Questions:
US-CERT Security Operations Center
Email: soc@us-cert.gov
Phone: 1-888-282-0870
Sponsored by
CISA





Exploit-DB query result for [Apache]





EXPLOIT
DATABASE



Exploit Database Advanced Search

Title

Apache

CVE

2021-1234

Type

Platform

Port

Content

Exploit content

Author

Author

Tag

Search
















☐ Verified

☐ Has App

☐ No Metasploit

Reset

Show 15

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