

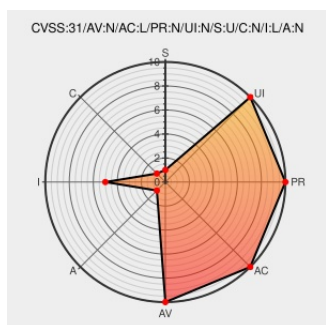


CVE-2021-33190

Published on: 06/08/2021 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:35:00 AM UTC

CVE-2021-33190

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

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

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

CVE-2021-33190 has been assigned by security@apache.org to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Apache Software Foundation - Apache APISIX Dashboard** version = 2.6

Vulnerability Patch/Work Around

1. Change the account password after installation, do not use the default password.
2. Upgrade to 2.6.1 or newer.

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

NONE

PARTIAL

NONE

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org text/html	 MLIST [apisix-dev] 20210608 CVE-2021-33190: Apache APISIX Dashboard: Bypass network access control
oss-security - CVE-2021-33190: Apache APISIX Dashboard: Bypass network access control	www.openwall.com text/html	 MLIST [oss-security] 20210608 CVE-2021-33190: Apache APISIX Dashboard: Bypass network access control

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	Apisix Dashboard	2.6	All	All	All
cpe:2.3:a:apache:apisix_dashboard:2.6:*****:.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-33190 : In #Apache APISIX Dashboard version 2.6, we changed the default value of listen host to 0.0.0.0 in... twitter.com/i/web/status/1...	2021-06-08 15:10:34
 /r/netcve	CVE-2021-33190	2021-06-08 15:41:48

[← 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 registered 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](#)