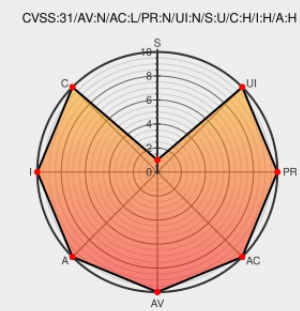
CVE-2021-45232

Published on: Not Yet Published

Last Modified on: 01/07/2022 01:45:00 PM UTC

CVE-2021-45232

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



Certain versions of Apisix Dashboard from Apache contain the following vulnerability:

In Apache APISIX Dashboard before 2.10.1, the Manager API uses two frameworks and introduces framework `droplet` on the basis of framework `gin`, all APIs and authentication middleware are developed based on framework `droplet`, but some API directly use the interface of framework `gin` thus bypassing the authentication.

CVE-2021-45232 has been assigned by security@apache.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache APISIX Dashboard** version **= 2.7 and 2.7.1**

Affected Vendor/Software: **Apache Software Foundation** - **Apache APISIX Dashboard** version **= 2.8**

Affected Vendor/Software: **Apache Software Foundation** - **Apache APISIX Dashboard** version **= 2.9**

Affected Vendor/Software: **Apache Software Foundation** - **Apache APISIX Dashboard** version **= 2.10**

Vulnerability Patch/Work Around

Implement one of the following mitigation techniques: 1. Upgrade to release 2.10.1 2. Change the default username and password, restrict the source IP to access the Apache APISIX Dashboard

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication

NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	lists.apache.org text/html	MISC lists.apache.org/thread/979qbl6vlm8269fopfyygnxofgqyn6k5
oss-security - CVE-2021-45232: Apache APISIX Dashboard: security vulnerability on unauthorized access	www.openwall.com text/html	MLIST [oss-security] 20211227 CVE-2021-45232: Apache APISIX Dashboard: security vulnerability on unauthorized access

Related QID Numbers

730323 Apache Apisix Remote Code Execution (RCE) Vulnerability

Exploit/POC from Github

CVE-2021-45232-RCE-多线程批量漏洞检测

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Apisix Dashboard	All	All	All	All

cpe:2.3:a:apache:apisix_dashboard:*:*:*:*:*:*:*:*:

Discovery Credit

Independently discovered by ZHU Yucheng of YuanbaoTeach Security Team.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-45232 : In #Apache APISIX Dashboard before 2.10.1, the Manager API uses two frameworks and introduces fram… twitter.com/i/web/status/1…	2021-12-27 15:10:50
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-45232 Description: In Apache APISIX Dashboard before 2.10.1, the Manage… twitter.com/i/web/status/1…	2021-12-27 15:56:12
@oss_security	CVE-2021-45232: Apache APISIX Dashboard: security vulnerability on unauthorized access: Posted by JunXu Chen on Dec… twitter.com/i/web/status/1…	2021-12-27 16:50:02

← Previous ID Next ID→

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