



CVE-2020-35846

Published on: 12/29/2020 12:00:00 AM UTC

Last Modified on: 09/02/2022 03:43:00 PM UTC

CVE-2020-35846

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

Certain versions of [Cockpit](#) from [Agentejo](#) contain the following vulnerability:

Agentejo Cockpit before 0.11.2 allows NoSQL injection via the Controller/Auth.php check function.

CVE-2020-35846 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

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
Cockpit	Product Vendor Advisory getcockpit.com text/html	MISC getcockpit.com/

 MISC
github.com/agentejo/cockpit/commit/79fc9631ffa29146e3124ceaf99879b92e1ef24b

 MISC
github.com/agentejo/cockpit/commit/33e7199575631ba1f74cba6b16b10c820bec59af

 [MISC packetstormsecurity.com/files/162282/Cockpit-CMS-0.11.1-NoSQL-Injection-Remote-Command-Execution.html](https://packetstormsecurity.com/files/162282/Cockpit-CMS-0.11.1-NoSQL-Injection-Remote-Command-Execution.html)

MISC
github.com/agentjo/cockpit/commit/2a385af8d80ed60d40d386ed813c1039db00c46f

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

Exploit/POC from Github

Cockpit CMS 0.11.1 NoSQL Injection to Remote Code Execution

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Agentejo	Cockpit	All	All	All	All
Application	Agentejo	Cockpit	All	All	All	All

```
cpe:2.3:a:agentejo:cockpit:*.:*:*:*:*:*:
```

```
cpe:2.3:a:agentejo:cockpit:*.:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @ipssignatures	It's new to me that Hillstone has a protection/signature/rule for the vulnerability CVE-2020-35846.... twitter.com/i/web/status/1...	2021-05-10 05:02:01
 @ipssignatures	It is the first time for me to know a protection/signature/rule for the vulnerability CVE-2020-35846. #Shp7xe4ypp7piw	2021-05-10 05:02:01
 @RemotelyAlerts	Severity: ??? Agentejo Cockpit before 0.11.2 allows No... CVE-2020-35846 Link for more: alerts.remotelyrmm.com/CVE-2020-35846	2022-09-02 17:35:02

@remotely-sec	https://remotely.mimic.com CVE-2020-35846	17:00:02
🐞 @LinInfoSec	Php - CVE-2020-35846: getcockpit.com	2022-09-02 18:02:57

← 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](#)