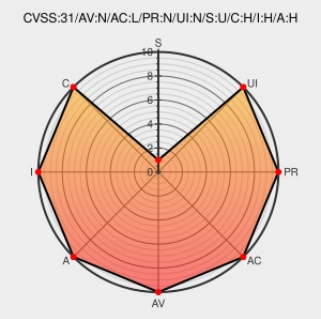
CVE-2020-35846

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 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/

fix possible security issue for login · agentejo/cockpit@79fc963 · GitHub	Patch Vendor Advisory github.com text/html	MISC github.com/agentejo/cockpit/commit/79fc9631ffa29146e3124ceaf99879b92e1ef24b
don't allow callable strings for $func (MongoLite) · agentejo/cockpit@33e7199 · GitHub	Patch Vendor Advisory github.com text/html	MISC github.com/agentejo/cockpit/commit/33e7199575631ba1f74cba6b16b10c820bec59af
Cockpit CMS 0.11.1 NoSQL Injection / Remote Command Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/162282/Cockpit-CMS-0.11.1-NoSQL-Injection-Remote-Command-Execution.html
remove $fn, $func, $f as field filter ... add $where as an alternativ… · agentejo/cockpit@2a385af · GitHub	Patch Vendor Advisory github.com text/html	MISC github.com/agentejo/cockpit/commit/2a385af8d80ed60d40d386ed813c1039db00c466

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

@RemotelyAlerts	alerts.remotelynmm.com/CVE-2020-35846	17:35:02
@LinInfoSec	Php - CVE-2020-35846: getcockpit.com	2022-09-02 18:02:57

← Previous ID

Next ID→