EXECUTIVE SOC TRIAGE REPORT: CVE-2020-35848

Date: October 30, 2025
Analyst: **Brandon**
Priority: **CRITICAL (P1)**

---

1. Executive Summary

A critical vulnerability, **CVE-2020-35848**, affecting Agentcjo Cockpit CMS, has been analyzed and triaged. Due to its **CVSS Base Score of 9.8** and confirmed **active exploitation in the wild (GreyNoise)**, immediate action is required to patch affected assets and contain observed attack vectors. The vulnerability is a NoSQL Injection flaw that allows for authentication bypass. The recommended immediate action is to deploy the vendor-supplied patch (version 0.11.2 or later).

2. Vulnerability Assessment

Core Findings

Detail	Value
CVE ID	**CVE-2020-35848**
CVSS Base Score	**9.8 (CRITICAL)**
Vulnerability Type	NoSQL Injection (Authentication Bypass)
Affected Component	Cockpit CMS (`Controller/Auth.php:newpassword` function)
Exploit Status	**Has Public Exploit: Yes** (Confirmed active exploitation by GreyNoise)

The vulnerability stems from improper input validation, allowing an attacker to manipulate database queries to gain unauthorized access to user accounts. This requires P1 priority for remediation.

3. Threat Intelligence & Proof of Concept (POC)

Threat Intelligence

Review of threat intelligence confirmed the critical nature, showing that **GreyNoise has detected active exploitation attempts in the wild**. This finding validates the severity rating and drives the need for urgent mitigation planning.

Proof of Concept (Scanner Use)

As part of the analysis workflow, remote reconnaissance was performed using an open-source scanner (URLScan.io) against a test asset (`http://testphp.vulnweb.com`). This demonstrated the capability to rapidly map a target's network details, such as IP (`44.228.249.3`) and hosting information (AMAZON-02). This tool integration is necessary for rapid asset identification prior to a confirmed attack.

4. Action Plan: Mitigation and Containment

IMMEDIATE ACTION IS REQUIRED by both the Patch Management and Network Operations teams.

Mitigation (Vulnerability Remediation)

- **P1: Immediate Patching:** The core vulnerability, **CVE-2020-35848**, must be eliminated by upgrading the Cockpit CMS to **version 0.11.2 or later**.
- **Vulnerability Remediation:** The patch focuses on improving **input validation** in the affected `newpassword` function, permanently eliminating the NoSQL injection flaw.
- **Asset Isolation:** All internal servers running the vulnerable Cockpit CMS must be **isolated** from public network access immediately until the patch is successfully deployed and verified.

Containment (Observed Attack Vector)

- **Network Containment:** Any observed attack source IP (e.g., as determined by AbuseIPDB checks) must be immediately **blocked** at the perimeter firewall. This action is justified by the high threat score and non-corporate hosting of malicious IPs, preventing further malicious activity.

5. Analyst Reflection

The project successfully simulated a high-stakes SOC triage event, emphasizing the critical link between **threat intelligence and decisive action**. Key skills demonstrated include the ability to prioritize an incident based on a **Critical CVSS 9.8 score** and confirmation of active exploitation. We also validated the practical use of open-source tools—from NVD for scoring to URLScan.io for reconnaissance—reinforcing the principle that effective security requires rapid analysis, data-driven prioritization, and swift implementation of both network containment and vendor patches.