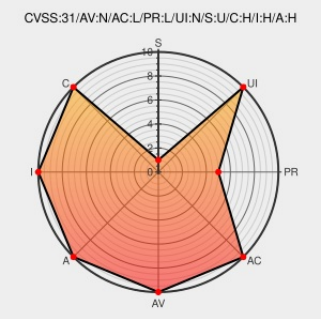
CVE-2021-39172

Published on: 08/27/2021 12:00:00 AM UTC

Last Modified on: 12/13/2022 04:51:00 PM UTC

CVE-2021-39172 - advisory for GHSA-9jxw-cfrh-jxq6

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



Certain versions of Catchet from Catchethq contain the following vulnerability:

Cachet is an open source status page system. Prior to version 2.5.1, authenticated users, regardless of their privileges (User or Admin), can exploit a new line injection in the configuration edition feature (e.g. mail settings) and gain arbitrary code execution on the server. This issue was addressed in version 2.5.1 by improving `UpdateConfigCommandHandler` and preventing the use of new lines characters in new configuration values. As a workaround, only allow trusted source IP addresses to access to the administration dashboard.

CVE-2021-39172 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **fiveai** - **Cachet** version **< 2.5.1**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

CVE References

Description	Tags	Link
Release v2.5.1 · fiveai/Cachet · GitHub	github.com text/html	MISC github.com/fiveai/Cachet/releases/tag/v2.5.1
Cachet 2.4: Code Execution via Laravel Configuration Injection	blog.sonarsource.com text/html	MISC blog.sonarsource.com/cachet-code-execution-via-laravel-configuration-injection/
New line injection during configuration edition · Advisory · fiveai/Cachet · GitHub	github.com text/html	CONFIRM github.com/fiveai/Cachet/security/advisories/GHSA-9jxw-cfrh-jxq6

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Catchethq	Catchet	All	All	All	All

cpe:2.3:a:catchethq:catchet:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-39172 : Cachet is an open source status page system. Prior to version 2.5.1, authenticated users, regardle… twitter.com/i/web/status/1…	2021-08-27 22:56:33
@SecRiskRptSME	RT: CVE-2021-39172 Cachet is an open source status page system. Prior to version 2.5.1, authenticated users, regar… twitter.com/i/web/status/1…	2021-08-29 07:33:39
@threatmeter	CVE-2021-39172 Cachet is an open source status page system. Prior to version 2.5.1, authenticated users, regardless… twitter.com/i/web/status/1…	2021-08-29 08:09:37

← Previous ID

Next ID→

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