

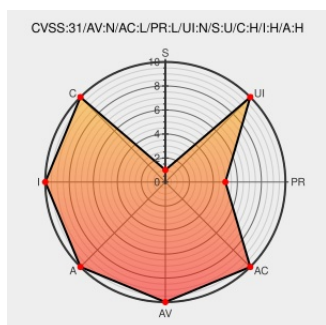


# CVE-2021-39172

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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>SINGLE</b>       |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

CVE References

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

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](mailto:comment@cve.report).

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 | <a href="#">Catchethq</a> | <a href="#">Catchet</a> | 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... <a href="#">twitter.com/i/web/status/1...</a> | 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... <a href="#">twitter.com/i/web/status/1...</a>  | 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... <a href="#">twitter.com/i/web/status/1...</a> | 2021-08-29 08:09:37 |

[← Previous ID](#)[Next ID →](#)

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](#)