

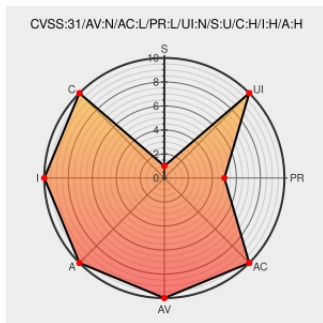


CVE-2021-39174

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

Last Modified on: 01/19/2023 02:58:00 AM UTC

CVE-2021-39174 - advisory for GHSA-88f9-7xxh-c688

[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 leak the value of any configuration entry of the dotenv file, e.g. the application secret (`APP\_KEY`) and various passwords (email, database, etc). This issue was addressed in version 2.5.1 by improving

`UpdateConfigCommandHandler` and preventing the use of nested variables in the resulting dotenv configuration file. As a workaround, only allow trusted source IP addresses to access to the administration dashboard.

CVE-2021-39174 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

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/
Configuration leak · Advisory · fiveai/Cachet · GitHub	github.com text/html	 CONFIRM github.com/fiveai/Cachet/security/advisories/GHSA-88f9-7xxh-c688

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

Cachet is an open source status page system. Prior to version 2.5.1, authenticated users, regardless of their privile...

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-2021-39174 : 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 23:30:15
 @SecRiskRptSME	RT: CVE-2021-39174 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 07:33:40
 @threatmeter	CVE-2021-39174 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 08:09:39
 @vuldb	Cachet up to 2.5.0 injection [CVE-2021-39174] vuldb.com/?id.181632	2021-08-30 06:58:32
 @threatmeter	Cachet up to 2.5.0 injection [CVE-2021-39174] A vulnerability, which was classified as critical, was found in Cache... twitter.com/i/web/status/1...	2021-08-30 09:50:40
 @0_g_u_z	@0x94	2021-08-30 18:04:36

© [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](#)