

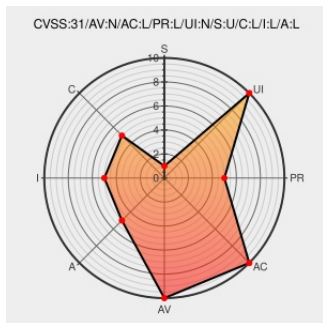


CVE-2022-29229

Published on: Not Yet Published

Last Modified on: 06/07/2022 02:28:00 PM UTC

CVE-2022-29229 - advisory for GHSA-7qcx-4p32-qcmx

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Competency And Skills System](#) from [Cassproject](#) contain the following vulnerability:

CaSS is a Competency and Skills System. CaSS Library, (npm:cassproject) has a missing cryptographic step when storing cryptographic keys that can allow a server administrator access to an account's cryptographic keys. This affects CaSS servers using standalone username/password authentication, which uses a method

that expects e2e cryptographic security of authorization credentials. The issue has been patched in 1.5.8, however, the vulnerable accounts are only resecured when the user next logs in using standalone authentication, as the data required to resecure the account is not available to the server. The issue may be mitigated by using SSO or client side certificates to log in. Please note that SSO and client side certificate authentication does not have this expectation of no-knowledge credential access, and cryptographic keys are available to the server administrator.

CVE-2022-29229 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [cassproject](#) - CASS version < 1.5.8

CVSS3 Score: **7.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	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 1.5.8: Merge remote-tracking branch 'origin/dependabot/npm_and_yarn/async-2....' · cassproject/CASS · GitHub	github.com text/html	MISC github.com/cassproject/CASS/releases/tag/1.5.8				
Missing Cryptographic Step in cassproject · Advisory · cassproject/CASS · GitHub	github.com text/html	CONFIRM github.com/cassproject/CASS/security/advisories/GHSA-7qcx-4p32-qcmx				
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						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Cassproject	Competency And Skills System	All	All	All	All
Application	Cassproject	Competency And Skills System	All	All	All	All
cpe:2.3:a:cassproject:competency_and_skills_system:*:*:*:*:docker:*:*:						
cpe:2.3:a:cassproject:competency_and_skills_system:*:*:*:*:node.js:*:*:						
No vendor comments have been submitted for this CVE						
Social Mentions						
Source	Title					Posted (UTC)
@CVEreport	CVE-2022-29229 : CaSS is a Competency and Skills System. CaSS Library, npm:cassproject has a missing cryptographi... twitter.com/i/web/status/1...					2022-05-18 21:01:12
@LinInfoSec	Npm - CVE-2022-29229: github.com/cassproject/CA...					2022-05-18 23:01:12
/r/netcve	CVE-2022-29229					2022-05-18 21:38:36
← 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](#)