VDB-355412 · CVE-2026-5622 · GCVE-100-355412

HCENGINEERING HULY PLATFORM 0.7.382 JWT TOKEN TOKEN.TS SERVER_SECRET HARD-CODED KEY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.4	$0-$5k	2.34-

Summary

A vulnerability categorized as problematic has been discovered in hcengineering Huly Platform 0.7.382. This affects an unknown part of the file *foundations/core/packages/token/src/token.ts* of the component *JWT Token Handler*. Such manipulation of the argument *SERVER_SECRET* with the input `secret` leads to hard-coded key. This vulnerability is uniquely identified as CVE-2026-5622. The attack can be launched remotely. Moreover, an exploit is present. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability, which was classified as problematic, has been found in hcengineering Huly Platform 0.7.382. Affected by this issue is an unknown functionality of the file *foundations/core/packages/token/src/token.ts* of the component *JWT Token Handler*. The manipulation of the argument `SERVER_SECRET` with the input value `secret` leads to a hard-coded key vulnerability. Using CWE to declare the problem leads to CWE-321. The use of a hard-coded cryptographic key significantly increases the possibility that encrypted data may be recovered. Impacted is integrity.

This vulnerability is handled as CVE-2026-5622. The exploitation is known to be difficult. The attack may be launched remotely. No form of authentication is required for exploitation. Technical details as well as a exploit are known. The MITRE ATT&CK project declares the attack technique as T1600.001.

It is declared as proof-of-concept. The vendor was contacted early about this disclosure but did not respond in any way.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Product

Vendor

- hcengineering

Name

- Huly Platform

Version

- 0.7.382

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 3.7
VulDB Meta Temp Score: 3.4

VulDB Base Score: 3.7
VulDB Temp Score: 3.4
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Hard-coded key
CWE: CWE-321 / CWE-320
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Status: Proof-of-Concept
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

04/05/2026		Advisory disclosed
04/05/2026	+0 days	VulDB entry created
04/05/2026	+0 days	VulDB entry last update

Sources

Status: Not defined

CVE: CVE-2026-5622 (🔒)
GCVE (CVE): GCVE-0-2026-5622
GCVE (VulDB): GCVE-100-355412
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/05/2026 06:11 PM
Changes: 04/05/2026 06:11 PM (55)
Complete: 🔍
Submitter: Ghufran Khan
Cache ID: 145:36D:179

Submit

Accepted

- Submit #785631: hcengineering platform v0.7.382 Authentication Bypass Issues (by Ghufran Khan)

Discussion

No comments yet. Languages: en.

Please log in to comment.