VDB-355413 · CVE-2026-5623 · GCVE-100-355413

HCENGINEERING HULY PLATFORM 0.7.382 IMPORT ENDPOINT INDEX.TS SERVER-SIDE REQUEST FORGERY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	2.01-

Summary

A vulnerability identified as critical has been detected in hcengineering Huly Platform 0.7.382. This vulnerability affects unknown code of the file *server/front/src/index.ts* of the component *Import Endpoint*. Performing a manipulation results in server-side request forgery. This vulnerability was named CVE-2026-5623. The attack may be initiated remotely. In addition, an exploit is available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability, which was classified as critical, was found in hcengineering Huly Platform 0.7.382. This affects some unknown functionality of the file *server/front/src/index.ts* of the component *Import Endpoint*. The manipulation with an unknown input leads to a server-side request forgery vulnerability. CWE is classifying the issue as CWE-918. The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination. This is going to have an impact on confidentiality, integrity, and availability.

This vulnerability is uniquely identified as CVE-2026-5623. The exploitability is told to be easy. It is possible to initiate the attack remotely. Technical details and a public exploit are known.

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: 6.3
VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒

VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Server-side request forgery
CWE: CWE-918
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
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-2026-5623 (🔒)
GCVE (CVE): GCVE-0-2026-5623
GCVE (VulDB): GCVE-100-355413
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/05/2026 06:11 PM
Changes: 04/05/2026 06:11 PM (54)
Complete: 🔍
Submitter: Ghufran Khan
Cache ID: 145:E8D:179

Submit

Accepted

- Submit #785632: hcengineering platform v0.7.382 Server-Side Request Forgery (by Ghufran Khan)

Discussion

No comments yet. Languages: en.

Please log in to comment.