VDB-355291 · CVE-2026-5538 · GCVE-100-355291

QINGDAOU ONLINEJUDGE UP TO 1.6.1 JUDGE_SERVER_HEARTBEAT ENDPOINT JUDGESERVER.SERVICE_URL SERVER-SIDE REQUEST FORGERY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
6.1	$0-$5k	2.69-

Summary

A vulnerability classified as critical has been found in QingdaoU OnlineJudge up to 1.6.1. This affects the function `service_url` of the file *JudgeServer.service_url* of the component *judge_server_heartbeat Endpoint*. This manipulation causes server-side request forgery. This vulnerability is handled as CVE-2026-5538. The attack can be initiated remotely. There is not any exploit available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability was found in QingdaoU OnlineJudge up to 1.6.1. It has been declared as critical. Affected by this vulnerability is the function `service_url` of the file *JudgeServer.service_url* of the component *judge_server_heartbeat Endpoint*. The manipulation with an unknown input leads to a server-side request forgery vulnerability. The CWE definition for the vulnerability is 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. As an impact it is known to affect confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is known as CVE-2026-5538. The exploitation appears to be easy. The attack can be launched remotely. Technical details of the vulnerability are known, but there is no available exploit. The pricing for an exploit might be around USD $0-$5k at the moment (estimation calculated on 04/04/2026).

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.

Entry connected to this vulnerability is available at VDB-123510.

Product

Vendor

- QingdaoU

Name

- OnlineJudge

Version

- 1.6.0
- 1.6.1

CPE 2.3

- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 6.1

VulDB Base Score: 6.3
VulDB Temp Score: 6.1
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: 🔒
Status: Not defined
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

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

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

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

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5538 (🔒)
GCVE (CVE): GCVE-0-2026-5538
GCVE (VulDB): GCVE-100-355291
See also: 🔒

Entry

Created: 04/04/2026 08:49 AM
Changes: 04/04/2026 08:49 AM (54)
Complete: 🔍
Submitter: Ana10gy
Cache ID: 52:90D:179

Submit

Accepted

- Submit #782203: QingdaoU OnlineJudge <=v1.6.1 Stored SSRF (by Ana10gy)

Discussion

No comments yet. Languages: en.

Please log in to comment.