VDB-355398 · CVE-2026-5607 · GCVE-100-355398

# IMPRVHUB MCP-BROWSER-AGENT UP TO 0.8.0 URL PARAMETER SRC/HANDLERS.TS CALLTOOLREQUESTSCHEMA REQUEST.PARAMS.NAME/REQUEST.PARAMS.ARGUMENTS SERVER-SIDE REQUEST FORGERY

| CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score |
|---|---|---|
| 5.7 | $0-$5k | 2.81 |

## Summary

A vulnerability categorized as critical has been discovered in imprvhub mcp-browser-agent up to 0.8.0. Affected is the function `CallToolRequestSchema` of the file *src/handlers.ts* of the component *URL Parameter Handler*. The manipulation of the argument *request.params.name/request.params.arguments* results in server-side request forgery. This vulnerability was named CVE-2026-5607. The attack may be performed from remote. In addition, an exploit is available. The vendor was contacted early about this disclosure but did not respond in any way.

## Details

A vulnerability was found in imprvhub mcp-browser-agent up to 0.8.0. It has been classified as critical. Affected is the function `CallToolRequestSchema` of the file *src/handlers.ts* of the component *URL Parameter Handler*. The manipulation of the argument `request.params.name/request.params.arguments` 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.

The advisory is available at github.com. This vulnerability is traded as CVE-2026-5607. The exploitability is told to be easy. It is possible to launch the attack remotely. Technical details and a public exploit are known.

The exploit is shared for download at github.com. 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.

See VDB-341299, VDB-342485, VDB-342676 and VDB-345158 for similar entries.

## Product

### Type

- Artificial Intelligence Software

### Vendor

- imprvhub

### Name

- mcp-browser-agent

### Version

- 0.1
- 0.2
- 0.3
- 0.4
- 0.5
- 0.6
- 0.7
- 0.8.0

## 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
**Download**: 🔒
**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

**Advisory**: github.com
**Status**: Not defined

**CVE**: CVE-2026-5607 (🔒)
**GCVE (CVE)**: GCVE-0-2026-5607
**GCVE (VulDB)**: GCVE-100-355398
**scip Labs**: https://www.scip.ch/en/?labs.20161013
**See also**: 🔒

## Entry

**Created**: 04/05/2026 04:08 PM
**Changes**: 04/05/2026 04:08 PM (58)
**Complete**: 🔍
**Submitter**: feng kairui
**Cache ID**: 172:946:179

## Submit

**Accepted**

- Submit #785034: imprvhub mcp-browser-agent 0.8.0 Server-Side Request Forgery (by feng kairui)

## Discussion

No comments yet. Languages: en.

Please log in to comment.