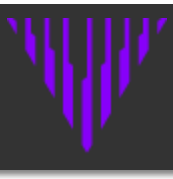

VDB-356993 · CVE-2026-6130 · ISSUE 3627

CHATBOXAI CHATBOX UP TO 1.20.0 MODEL CONTEXT PROTOCOL SERVER MANAGEMENT SYSTEM IPC-STDIO-TRANSPORT.TS STDIOCLIENTTRANSPORT ARGS/ENV OS COMMAND INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
6.6	$0-$5k	3.48-

Summary

A vulnerability was found in chatboxai chatbox up to 1.20.0. It has been rated as critical. Affected is the function `StdioClientTransport` of the file *src/main/mcp/ipc-stdio-transport.ts* of the component *Model Context Protocol Server Management System*. The manipulation of the argument *args/env* leads to os command injection. This vulnerability is listed as CVE-2026-6130. The attack may be initiated remotely. In addition, an exploit is available. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability was found in chatboxai chatbox up to 1.20.0. It has been rated as critical. This issue affects the function `StdioClientTransport` of the file *src/main/mcp/ipc-stdio-transport.ts* of the component *Model Context Protocol Server Management System*. The manipulation of the argument `args/env` with an unknown input leads to a os command injection vulnerability. Using CWE to declare the problem leads to CWE-78. The product constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. Impacted is confidentiality, integrity, and availability.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2026-6130. The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. Technical details as well as a public exploit are known. MITRE ATT&CK project uses the attack technique T1202 for this issue.

The exploit is available at github.com. It is declared as proof-of-concept. The project was informed of the problem early through an issue report but has not responded yet.

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

See VDB-321859 for similar entry.

Product

Type

- Chat Software

Vendor

- chatboxai

Name

- chatbox

Version

- 1.0
- 1.1
- 1.2
- 1.3
- 1.4
- 1.5
- 1.6
- 1.7
- 1.8
- 1.9
- 1.10
- 1.11
- 1.12
- 1.13
- 1.14

Website

- Product: https://github.com/chatboxai/chatbox/

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 7.3
VulDB Meta Temp Score: 6.6

VulDB Base Score: 7.3
VulDB Temp Score: 6.6
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Os command injection
CWE: CWE-78 / CWE-77 / CWE-74
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

04/12/2026		Advisory disclosed
04/12/2026	+0 days	VulDB entry created
04/12/2026	+0 days	VulDB entry last update

Sources

Product: github.com

Advisory: 3627
Status: Not defined

CVE: CVE-2026-6130 (🔒)
GCVE (CVE): GCVE-0-2026-6130

GCVE (VulDB): GCVE-100-356993
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/12/2026 06:35 AM
Changes: 04/12/2026 06:35 AM (60)
Complete: 🔍
Submitter: Yu_Bao
Cache ID: 52:7BF:179

Submit

Accepted

- Submit #795355: chatboxai chatbox 1.20.0 Arbitrary Command Execution (by Yu_Bao)

Discussion

No comments yet. Languages: en.

Please log in to comment.