



VDB-355327 · CVE-2026-5557 · GCVE-100-355327

# BADLOGIC PI-MONO UP TO 0.58.4 PI-MOM SLACK BOT SLACK.TS AUTHENTICATION BYPASS

CVSS Meta Temp Score ⓘ

5.7

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

1.84-

## Summary

A vulnerability was found in [badlogic pi-mono up to 0.58.4](#). It has been rated as **critical**. Impacted is an unknown function of the file `packages/mom/src/slack.ts` of the component *pi-mom Slack Bot*. This manipulation causes authentication bypass. This vulnerability is tracked as [CVE-2026-5557](#). The attack is possible to be carried out remotely. Moreover, an exploit is present. The vendor was contacted early about this disclosure but did not respond in any way.

## Details

A vulnerability was found in [badlogic pi-mono up to 0.58.4](#). It has been declared as **critical**. Affected by this vulnerability is an unknown function of the file `packages/mom/src/slack.ts` of the component *pi-mom Slack Bot*. The manipulation with an unknown input leads to a authentication bypass vulnerability. The CWE definition for the vulnerability is [CWE-288](#). A product requires authentication, but the product has an alternate path or channel that does not require authentication. 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-2026-5557](#). The exploitation appears to be easy. The attack can be launched remotely. Technical details and also a public exploit are known.

It is possible to download the exploit 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.

The entries [VDB-355286](#) and [VDB-355326](#) are pretty similar.

## Product

### Vendor

- [badlogic](#)

### Name

- [pi-mono](#)



### Version

- [0.58.0](#)
- [0.58.1](#)
- [0.58.2](#)
- [0.58.3](#)
- [0.58.4](#)


## 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: Authentication bypass  
CWE: [CWE-288](#) / [CWE-287](#)  
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

04/04/2026		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-2026-5557](#) (🔒)

**GCVE (CVE):** [GCVE-0-2026-5557](#)

**GCVE (VulDB):** [GCVE-100-355327](#)

**scip Labs:** <https://www.scip.ch/en/?labs.20161013>

**See also:** 🔒

## Entry

**Created:** 04/04/2026 03:55 PM

**Changes:** 04/04/2026 03:55 PM (56)

**Complete:** 🔍

**Submitter:** [Yu Bao](#)

**Cache ID:** 74:724:179

## Submit

**Accepted**

- [Submit #782879](#): badlogic pi-mono 0.58.4 Unauthenticated Remote Code Execution (by Yu Bao)

## Discussion

No comments yet. Languages: en.

Please [log in](#) to comment.

