VDB-355286 · CVE-2026-5533 · GCVE-100-355286

BADLOGIC PI-MONO 0.58.4 SVG ARTIFACT SVGARTIFACT.TS CROSS SITE SCRIPTING

CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score

3.9 | $0-$5k | 1.86

Summary

A vulnerability categorized as problematic has been discovered in badlogic pi-mono 0.58.4. This affects an unknown function of the file *packages/web-ui/src/tools/artifacts/SvgArtifact.ts* of the component *SVG Artifact Handler*. Such manipulation leads to cross site scripting. This vulnerability is documented as CVE-2026-5533. The attack can be executed remotely. Additionally, an exploit exists. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability, which was classified as problematic, has been found in badlogic pi-mono 0.58.4. Affected by this issue is an unknown functionality of the file *packages/web-ui/src/tools/artifacts/SvgArtifact.ts* of the component *SVG Artifact Handler*. The manipulation with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-79. The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. Impacted is integrity.

The advisory is available at github.com. This vulnerability is handled as CVE-2026-5533. The exploitation is known to be easy. The attack may be launched remotely. No form of authentication is required for exploitation. Successful exploitation requires user interaction by the victim. Technical details as well as a public exploit are known. This vulnerability is assigned to T1059.007 by the MITRE ATT&CK project.

The exploit is available 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.

Product

Vendor

- badlogic

Name

- pi-mono

Version

- 0.58.4

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 4.3
VulDB Meta Temp Score: 3.9

VulDB Base Score: 4.3
VulDB Temp Score: 3.9
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Cross site scripting
CWE: CWE-79 / CWE-94 / 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

04/04/2026		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-2026-5533 (🔒)
GCVE (CVE): GCVE-0-2026-5533
GCVE (VulDB): GCVE-100-355286
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/04/2026 08:40 AM
Changes: 04/04/2026 08:40 AM (56)
Complete: 🔍
Submitter: Yu Bao
Cache ID: 128:527:179

Submit

Accepted

- Submit #782170: Mario Zechner pi-mono 0.58.4 SVG Artifact Stored XSS Leading to Credential Theft (by Yu Bao)

Discussion

No comments yet. Languages: en.

Please log in to comment.