VDB-355329 · CVE-2026-5559 · GCVE-100-355329

ANTARESMUGISHO PYBLADE 0.1.8-ALPHA/0.1.9-ALPHA AST VALIDATION SANDBOX.PY _IS_SAFE_AST SPECIAL ELEMENTS USED IN A TEMPLATE ENGINE

Summary

A vulnerability identified as critical has been detected in AntaresMugisho PyBlade 0.1.8-alpha/0.1.9-alpha. The impacted element is the function `_is_safe_ast` of the file *sandbox.py* of the component *AST Validation*. Performing a manipulation results in improper neutralization of special elements used in a template engine. This vulnerability is cataloged as CVE-2026-5559. It is possible to initiate the attack remotely. Furthermore, there is an exploit available. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability classified as critical has been found in AntaresMugisho PyBlade 0.1.8-alpha/0.1.9-alpha. This affects the function `_is_safe_ast` of the file *sandbox.py* of the component *AST Validation*. The manipulation with an unknown input leads to a improper neutralization of special elements used in a template engine vulnerability. CWE is classifying the issue as CWE-1336. The product uses a template engine to insert or process externally-influenced input, but it does not neutralize or incorrectly neutralizes special elements or syntax that can be interpreted as template expressions or other code directives when processed by the engine. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is shared at github.com. This vulnerability is uniquely identified as CVE-2026-5559. The exploitability is told to be easy. It is possible to initiate the attack remotely. Technical details and a public exploit are known. MITRE ATT&CK project uses the attack technique T1221 for this issue.

The exploit is shared for download 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.

Product

Vendor

- AntaresMugisho

Name

- PyBlade

Version

- 0.1.8-alpha
- 0.1.9-alpha

Website

- Product: https://github.com/AntaresMugisho/PyBlade/

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: Improper neutralization of special elements used in a template engine
CWE: CWE-1336 / CWE-791 / CWE-790
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

Product: github.com

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5559 (🔒)
GCVE (CVE): GCVE-0-2026-5559
GCVE (VulDB): GCVE-100-355329
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/04/2026 03:59 PM
Changes: 04/04/2026 03:59 PM (57)
Complete: 🔍
Submitter: zhangxinyu06
Cache ID: 52:F69:179

Submit

Accepted

- Submit #782904: AntaresMugisho PyBlade v0.1.8-alpha through v0.2.0-alph Code Injection (by zhangxinyu06)

Discussion

No comments yet. Languages: en.

Please log in to comment.