VDB-355332 · CVE-2026-5562 · GCVE-100-355332

PROVECTUS KAFKA-UI UP TO 0.7.2 ENDPOINT TESTEXECUTIONS VALIDATEACCESS CODE INJECTION

Summary

A vulnerability described as critical has been identified in provectus kafka-ui up to 0.7.2. Affected is the function `validateAccess` of the file */api/smartfilters/testexecutions* of the component *Endpoint*. The manipulation results in code injection. This vulnerability is reported as CVE-2026-5562. The attack can be launched remotely. Moreover, an exploit is present. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability, which was classified as critical, was found in provectus kafka-ui up to 0.7.2. Affected is the function `validateAccess` of the file */api/smartfilters/testexecutions* of the component *Endpoint*. The manipulation with an unknown input leads to a code injection vulnerability. CWE is classifying the issue as CWE-94. The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is shared for download at drive.google.com. This vulnerability is traded as CVE-2026-5562. The exploitability is told to be easy. It is possible to launch the attack remotely. The exploitation doesn't require any form of authentication. Technical details and a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1059.

The exploit is shared for download at drive.google.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-354512, VDB-354543, VDB-354548 and VDB-354549 are pretty similar.

Product

Vendor

- provectus

Name

- kafka-ui

Version

- 0.7.0
- 0.7.1
- 0.7.2

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: Code injection
CWE: CWE-94 / CWE-74 / CWE-707
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: drive.google.com
Status: Not defined

CVE: CVE-2026-5562 (🔒)
GCVE (CVE): GCVE-0-2026-5562
GCVE (VulDB): GCVE-100-355332
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/04/2026 04:12 PM
Changes: 04/04/2026 04:12 PM (57)
Complete: 🔍
Submitter: 0xNayel
Cache ID: 20:68C:179

Submit

Accepted

- Submit #782941: https://github.com/provectus/ kafka-ui 0.7.2 Code Injection (by 0xNayel)

Discussion

No comments yet. Languages: en.

Please log in to comment.