VDB-355338 · CVE-2026-5568 · GCVE-100-355338

AKAUNTING UP TO 3.1.21 INVOICE/BILLING NOTES CROSS SITE SCRIPTING

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.2	$0-$5k	1.86-

Summary

A vulnerability was found in Akaunting up to 3.1.21 and classified as problematic. Impacted is an unknown function of the component *Invoice/Billing*. The manipulation of the argument *notes* results in cross site scripting. This vulnerability was named CVE-2026-5568. The attack may be performed from remote. In addition, an exploit is available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability classified as problematic has been found in Akaunting up to 3.1.21. Affected is an unknown code of the component *Invoice/Billing*. The manipulation of the argument `notes` with an unknown input leads to a cross site scripting vulnerability. CWE is classifying the issue as 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. This is going to have an impact on integrity.

The advisory is available at docs.google.com. This vulnerability is traded as CVE-2026-5568. The exploitability is told to be easy. It is possible to launch the attack remotely. Successful exploitation requires user interaction by the victim. Technical details and a public exploit are known. This vulnerability is assigned to T1059.007 by the MITRE ATT&CK project.

The exploit is shared for download at docs.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.

See VDB-216741, VDB-278200, VDB-289181 and VDB-312000 for similar entries.

Product

Name

- Akaunting

Version

- 3.1.0
- 3.1.1
- 3.1.2
- 3.1.3
- 3.1.4
- 3.1.5
- 3.1.6
- 3.1.7
- 3.1.8
- 3.1.9
- 3.1.10
- 3.1.11
- 3.1.12
- 3.1.13
- 3.1.14

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 3.5
VulDB Meta Temp Score: 3.2

VulDB Base Score: 3.5
VulDB Temp Score: 3.2

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: docs.google.com
Status: Not defined

CVE: CVE-2026-5568 (🔒)
GCVE (CVE): GCVE-0-2026-5568
GCVE (VulDB): GCVE-100-355338
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/04/2026 04:34 PM
Changes: 04/04/2026 04:34 PM (55)
Complete: 🔍
Submitter: gabriel
Cache ID: 20:32F:179

Submit

Accepted

- Submit #783139: Akaunting v3.1.21 Cross Site Scripting (by gabriel)

Discussion

No comments yet. Languages: en.

Please log in to comment.