VDB-354443 · CVE-2026-5253 · GCVE-100-354443

BUFANYUN HOTGO 1.0/2.0 EDITNOTICE ENDPOINT MESSAGELIST.VUE CROSS SITE SCRIPTING

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.2	$0-$5k	1.61-

Summary

A vulnerability was found in bufanyun HotGo 1.0/2.0. It has been classified as problematic. Affected by this issue is some unknown functionality of the file */web/src/layout/components/Header/MessageList.vue* of the component *editNotice Endpoint*. The manipulation leads to cross site scripting. This vulnerability is listed as CVE-2026-5253. The attack may be initiated remotely. In addition, an exploit is available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability was found in bufanyun HotGo 1.0/2.0 and classified as problematic. This issue affects an unknown code block of the file */web/src/layout/components/Header/MessageList.vue* of the component *editNotice Endpoint*. 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.

It is possible to read the advisory at github.com. The identification of this vulnerability is CVE-2026-5253. The exploitation is known to be easy. The attack may be initiated remotely. It demands that the victim is doing some kind of user interaction. Technical details as well as a public exploit are known. The attack technique deployed by this issue is T1059.007 according to MITRE ATT&CK.

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.

See VDB-349585 for similar entry.

Product

Vendor

- bufanyun

Name

- HotGo

Version

- 1.0
- 2.0

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

03/31/2026		Advisory disclosed
03/31/2026	+0 days	VulDB entry created
03/31/2026	+0 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5253 (🔒)
GCVE (CVE): GCVE-0-2026-5253
GCVE (VulDB): GCVE-100-354443
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/31/2026 06:18 PM
Changes: 03/31/2026 06:18 PM (56)
Complete: 🔍
Cache ID: 74:BF9:179

Submit

Accepted

- Submit #780614: bufanyun HotGo <= v2.0 Cross Site Scripting (by github.com)

Discussion

No comments yet. Languages: en.

Please log in to comment.