



VDB-354449 · CVE-2026-5259 · GCVE-100-354449

AUTOHOMECORP FROSTMOURNE UP TO 1.0 ALARM PREVIEW ALARMCONTROLLER.JAVA SERVER-SIDE REQUEST FORGERY

CVSS Meta Temp Score

5.7

Current Exploit Price (≈)

\$0-\$5k

CTI Interest Score

3.09-

Summary

A vulnerability marked as **critical** has been reported in [AutohomeCorp frostmourne up to 1.0](#). The impacted element is an unknown function of the file `frostmourne-monitor/src/main/java/com/autohome/frostmourne/monitor/controller/AlarmController.java` of the component *Alarm Preview*. The manipulation leads to server-side request forgery. This vulnerability is traded as [CVE-2026-5259](#). It is possible to initiate the attack remotely. Furthermore, there is an exploit available.

Details

A vulnerability, which was classified as **critical**, has been found in [AutohomeCorp frostmourne up to 1.0](#). This issue affects an unknown code of the file `frostmourne-monitor/src/main/java/com/autohome/frostmourne/monitor/controller/AlarmController.java` of the component *Alarm Preview*. The manipulation with an unknown input leads to a server-side request forgery vulnerability. Using CWE to declare the problem leads to [CWE-918](#). The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination. Impacted is confidentiality, integrity, and availability.

The advisory is shared at [fx4tqqfvdw4.feishu.cn](#). The identification of this vulnerability is [CVE-2026-5259](#). The exploitation is known to be easy. The attack may be initiated remotely. Technical details as well as a public exploit are known.

The exploit is available at [fx4tqqfvdw4.feishu.cn](#). It is declared as proof-of-concept.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

The entry [VDB-350397](#) is related to this item.

Product

Vendor

- [AutohomeCorp](#)

Name

- [frostmourne](#)

Version

- [1.0](#)

CPE 2.3

- 

CPE 2.2

- 

CVSSv4

VuIDB Vector: 

VuIDB Reliability: 

CVSSv3

VuIDB Meta Base Score: 6.3

VuIDB Meta Temp Score: 5.7

VuIDB Base Score: 6.3

VuIDB Temp Score: 5.7

VuIDB Vector: 

VuIDB Reliability: 

CVSSv2

VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting

Class: Server-side request forgery

CWE: [CWE-918](#)

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: fx4tqqfvdw4.feishu.cn

Status: Not defined

CVE: [CVE-2026-5259](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5259](#)

GCVE (VulDB): [GCVE-100-354449](#)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

See also: 🔒

Entry

Created: 03/31/2026 06:27 PM

Changes: 03/31/2026 06:27 PM (55)

Complete: 🔍

Submitter: [xcxr](#)

Cache ID: 20:15B:179

Submit

Accepted

- [Submit #780669](#): AutohomeCorp frostmourne frostmourne <= 1.0 Server-Side Request Forgery (by xcxr)

Discussion

No comments yet. Languages: en.

Please log in to comment.