

[Server-Side Request Forgery i...](#)

## Description

SSRF via Alarm Preview Endp...

## Proof of Concept:

Prerequisites:

Step 1: Obtain Authentication T...

Step 2: Exploit SSRF

# Server-Side Request Forgery Alarm Preview

**BUG\_Author:** Chengxin Xu**Affected Version:** Frostmourne 1.0 (frostmourne-master)**Vendor:** [Frostmourne GitHub Repository](#)**Software:** [Frostmourne](#)**Vulnerability Files:**

- `frostmourne-monitor/src/main/java/com/autohome/frostmou  
java`
- `frostmourne-monitor/src/main/java/com/autohome/frostmou  
inService.java`
- `frostmourne-monitor/src/main/java/com/autohome/frostmou  
tpMetric.java`

## Description

Frostmourne contains a Server-Side Request Forgery (SSRF) `/alarm/previewData` endpoint allows authenticated use server without any URL validation and **returns the HTTP res** access internal network resources, cloud metadata endpoints

## SSRF via Alarm Preview Endpoint (`/api/monitc`

The vulnerability starts from the `AlarmController.previewData` `dataName` set to "http", the request flows through multiple I

**Entry Point (`AlarmController.java:55-76`):**