

Denial of Service through Logs in zoneminder

Moderate connortechonology published GHSA-cfcx-v52x-jh74 on Oct 7

Package

zoneminder (ZoneMinder)

Affected versions

<= 1.36.26, <= 1.37.23

Patched versions

1.36.27, 1.37.24

Description

Impact

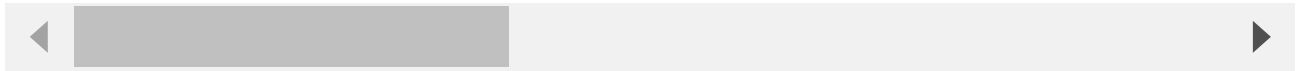
This is a potential Denial Of Service vulnerability.

Vulnerability allows users with "View" system permissions to inject data into the logs stored by Zoneminder. This was observed through an HTTP POST request containing log information to the "/zm/index.php" endpoint. Submission is not rate controlled and could affect database performance and/or consume all storage resources.

Example Request

```
POST /zm/index.php HTTP/1.1
Host: 10.0.10.107
Content-Length: 256
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://10.0.10.107
Referer: http://10.0.10.107/zm/?
Content-Security-Policy: default-src 'self' data: *; connect-src 'self'; script-src 'self';
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: zmSkin=classic; zmCSS=base; zmBandwidth=high; ZMSSID=8o8h3mg4nv7pmm4tm13r1v4d
Connection: close
```

__csrf_magic=key%3A85866fbc6a1d7325544a55aa63fb534677f34ca%2C1665102411&view=request&request=lo



Patches

[de2866f](#)

[73d9f24](#)

[cb3fc59](#)

[34ffd92](#)

Workarounds

Not at this time.

For more information

If you have any questions or comments about this advisory:

- Open an issue in <https://github.com/ZoneMinder/zoneminder>
- Email us at info@zoneminder.com

Severity

Moderate 4.3 / 10

CVSS base metrics

<u>Attack vector</u>	Network
<u>Attack complexity</u>	Low
<u>Privileges required</u>	Low
<u>User interaction</u>	None
<u>Scope</u>	Unchanged
<u>Confidentiality</u>	None
<u>Integrity</u>	None
<u>Availability</u>	Low

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L

CVE ID

CVE-2022-39291

Weaknesses

CWE-400

Credits

 trenchesofit