

# STORED XSS IN RITTAL CMC III

**Authors:** Álvaro Santos García and Miguel Haro Maldonado

**Application:** Rittal CMC PU III Web management

**Devices:** CMC PU III 7030.000

**Software Revision:** V3.11.00\_2

**Hardware Revision:** V3.00

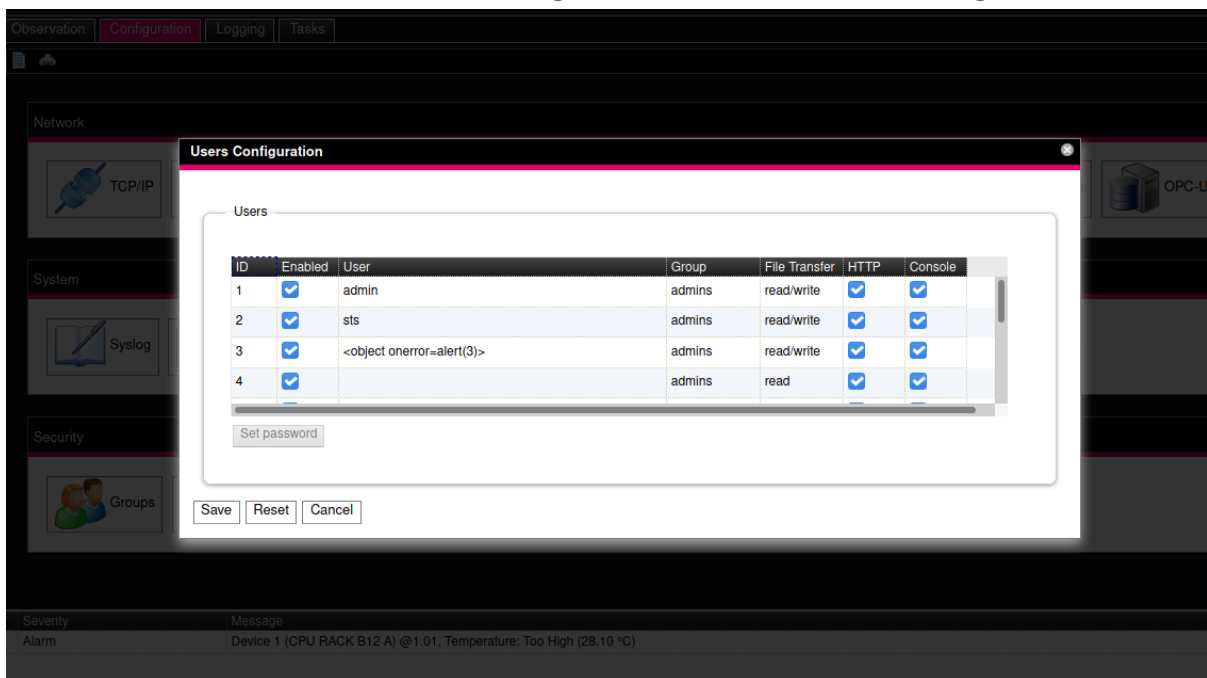
**Attack type:** Stored XSS

**Summary:** Web application fails to sanitize user input on Security User configuration dialog and Task tab. This flaw allows the attacker to inject HTML or browser interpreted content in the web application. In this case, the XSS of the user configuration will be displayed when the authentication is performed and also in the logs. The XSS of the task will also be interpreted in the log section. It is interesting to remark that both XSS will be persistent in the logs until they are deleted, even if the rogue input values are changed to correct ones. Successful exploitation requires access to the web management interface with a valid or hijacked session.

## Technical Description

To access the vulnerability, the user has to authenticate and have access to the configuration page.

## PROCESSING UNIT > Configuration Tab > User Configuration

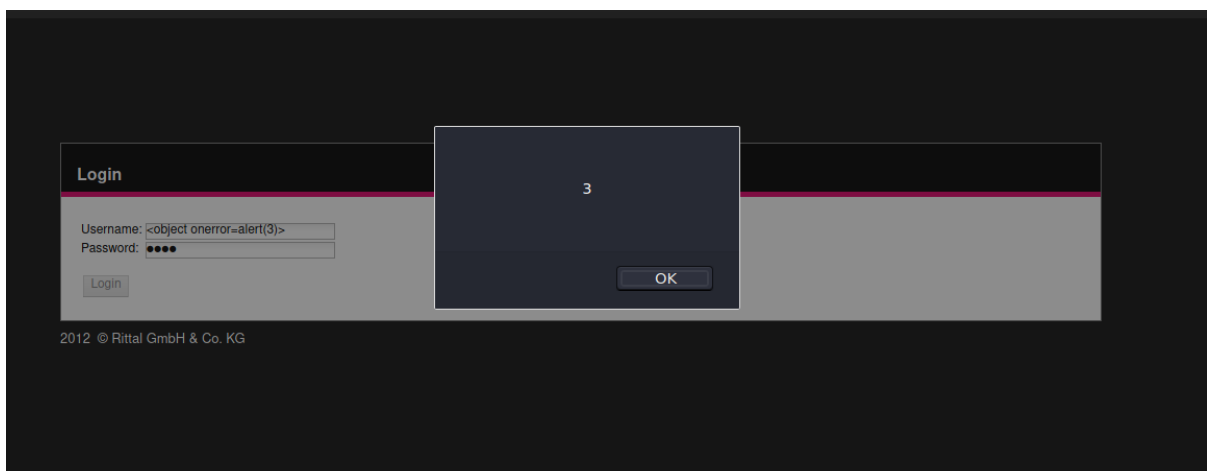


Field "User" is vulnerable to XSS. This field is protected against XSS strings and usernames larger than 20 characters, but with a proxy those defenses can be bypassed because they are triggered at client side.

A possible payload that works is the following:

```
<object onerror=alert(3)>
```

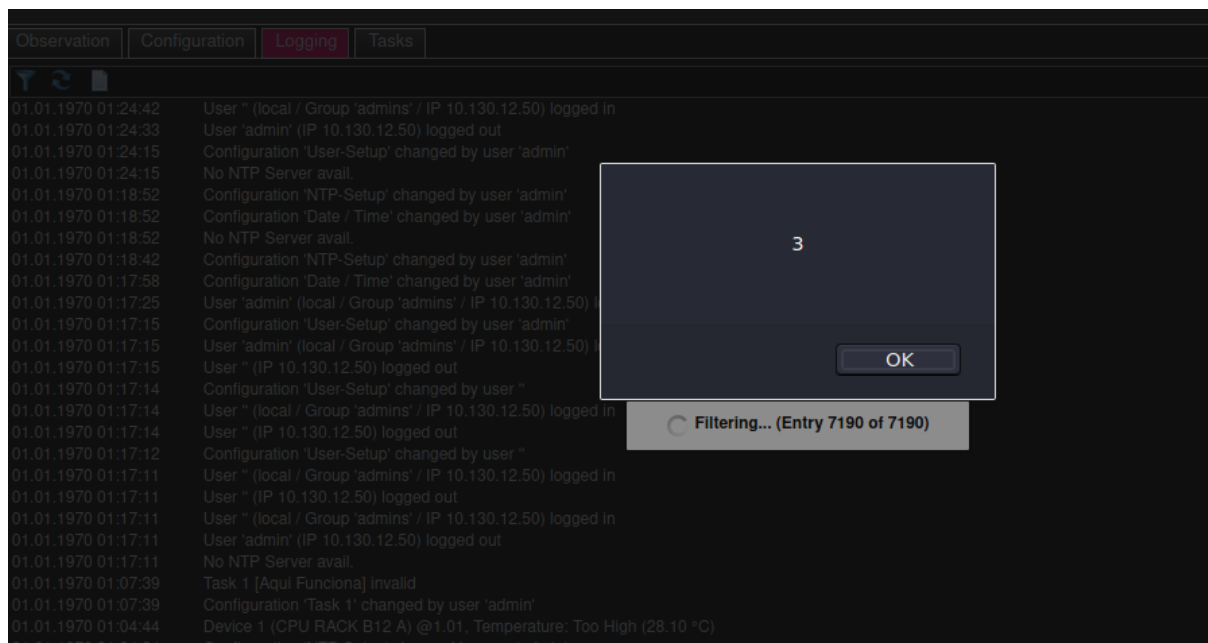
Once the user is created, we can login and the alert shows up.



Note that the user is also created inside the device.

```
(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
10.130.12.217: inverse host lookup failed: Host name lookup failure
connect to [10.130.12.50] from (UNKNOWN) [10.130.12.217] 59905
cat /etc/passwd
root:x:0:0:Super-User:/:/bin/sh
bin:x:1:1:bin:/bin:/bin/sh
daemon:x:2:2:Daemon:/sbin:/bin/sh
nobody:x:65534:65534:nobody:/var/lib/nobody:/bin/sh
sshd:x:65535:65534:sshd:/dev/null:/bin/false
admin:x:1000:1000:"CMC-User 1":/home/cmc:/bin/sh
sts:x:1001:1000:"CMC-User 2":/home/cmc:/bin/sh
<object onerror=alert(3)>x:1002:1000:"CMC-User 3":/home/cmc:/bin/sh
```

Everytime a user logs in or out, it creates a log that can be accessible in the Logging Tab. Here, the XSS is also stored using the name of the user. It will be executed every time a user accesses the Loggin Tab until the logs are deleted.



This stored XSS can also be created in the Task Tab, editing one task.

**Rittal CMC III PU**  
 Username: **admin**  

Password

Logout

Name : Aaaaaaaa  
 Location : Bbbbbbb  
 Contact : Cccccc  
 IP Address : 10.130.12.217

Processing Unit  
 Real Devices  
 [1] CPU RACK B12 A (CMCIII-PU)  
 Virtual Devices

Observation
 Configuration
 Logging
 **Tasks**

ID	Name	Description
1	<object onerror=alert(3)>	
2	Task 2	
3	Task 3	
4	Task 4	
5	Task 5	
6	Task 6	
7	Task 7	
8	Task 8	
9	Task 9	
10	Task 10	
11	Task 11	
12	Task 12	
13	Task 13	
14	Task 14	
15	Task 15	
16	Task 16	

The procedure is the same, inserting the XSS payload with a proxy, as the sanitizing actions are done at client side.

## PROCESSING UNIT > Task Tab > Edit Task

Observation
 Configuration
 Logging
 **Tasks**

ID	Name	Description
1	<object onerror=alert(3)>	
2	Prueba 2	
3	Task 3	
4	Task 4	
5	Task 5	
6	Task 6	
7	Task 7	
8	Task 8	
9	Task 9	
10	Task 10	
11	Task 11	
12	Task 12	
13	Task 13	
14	Task 14	
15	Task 15	
16	Task 16	

Task Configuration

Details

Enable ☐

Name

Description

None

Setup

Trigger Expression

-

No variable selected

No value

Save

Clear

Cancel

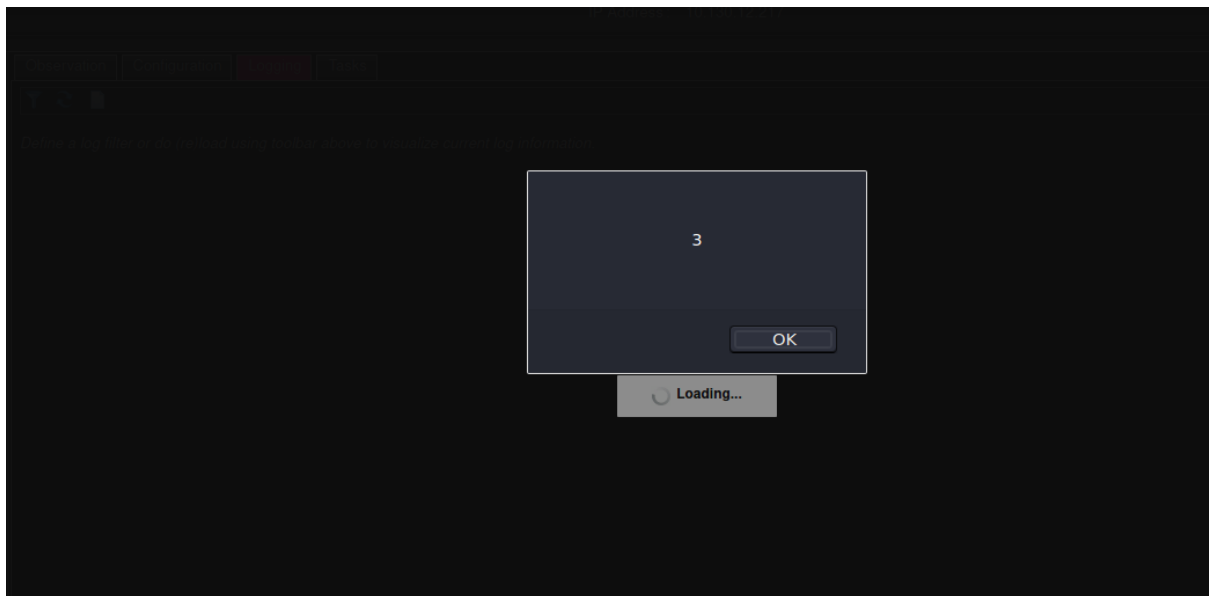
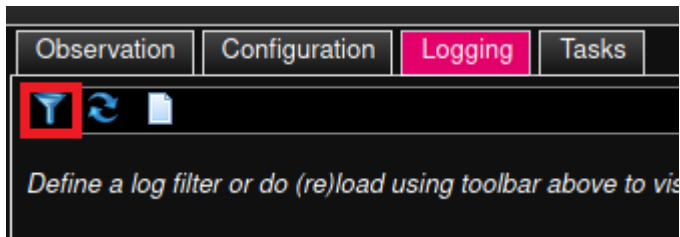
Severity

Message

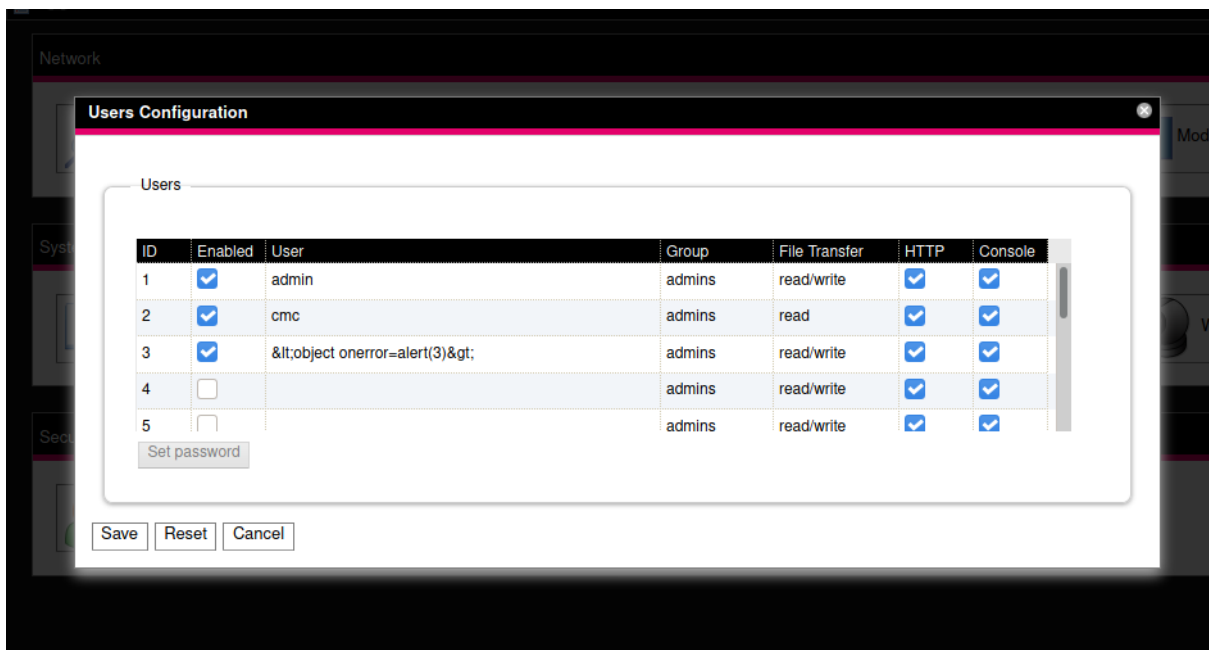
Alarm

Device 1 (CPU RACK B12 A) @1.01. Temperature: Too High (28.10 °C)

Again, accessing the Logging Tab, as seen in the stored XSS at user configuration, will trigger this stored XSS created in the Task Configuration. Clicking on the log filter icon will also trigger it. Below we show the results of clicking it.



From software V3.17.10 these vulnerabilities are patched, as the browser does not interpret HTML or JS code. Rogue strings can be inserted but not interpreted. The user field is encoded and no alert jumps when the user logs in.



**Rittal CMC III PU**  
 Username: &lt;object onerror=alert(3)&gt;  

Password

Logout

Name : <object onerror=alert(1)>  
 Location : Location of the Unit  
 Contact : Contact Person  
 IP Address : 10.130.12.218

The behaviour is the same in the Logging tab and using the logging filter. The XSS is controlled.

Monitoring
 Configuration
 **Logging**
 Tasks
 Charts
 Dashboards

01.01.1970 01:10:54

WARNING: This line replaces an invalid log entry (maybe the system was powered-down during logging the entry)

01.01.1970 01:09:57

Configuration of Dashboard 1 changed by user 'admin' [Web]

01.01.1970 01:09:57

Configuration of Task 1 changed by user 'admin' [Web]

01.01.1970 01:09:11

WARNING: This line replaces an invalid log entry (maybe the system was powered-down during logging the entry)

01.01.1970 01:09:11

Configuration of Task 1 changed by user 'admin' [Web]

01.01.1970 01:09:11

WARNING: This line replaces an invalid log entry (maybe the system was powered-down during logging the entry)

Set logging filter

Date	Type	Device Index	User	IP Address
All items	All items	All items	All items	All items
30.11.1899	Alarm	0	<;BODY ONLOAD=alert(';XSS');>;	10.128.10.153
08.10.2020	Device	1	<object onerror=alert(1)>	10.128.64.28
05.10.2020	Event	2	<object onerror=alert(3)>	10.128.64.46

Ok

Cancel