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

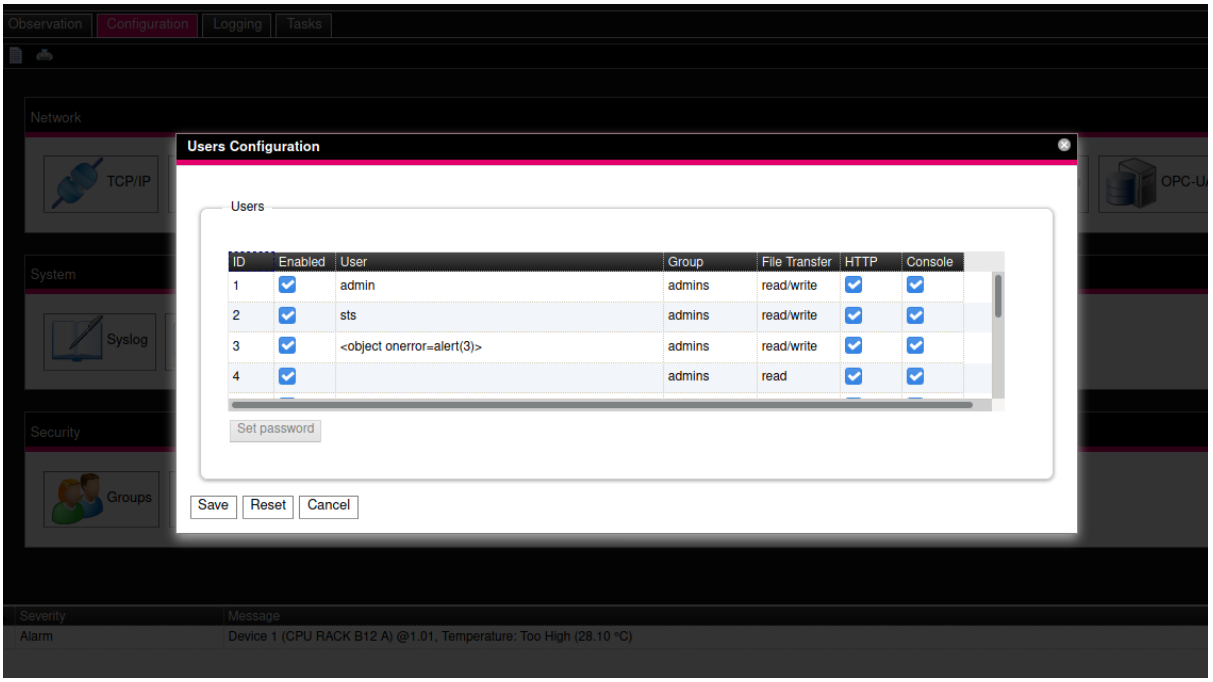
Attack type: Stored XSS

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

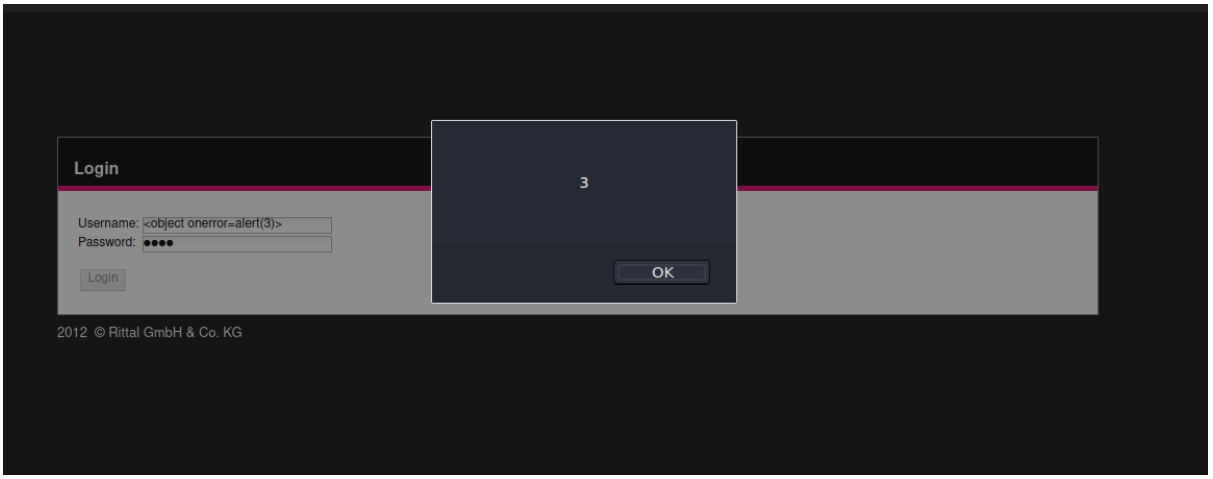


Field “User” is vulnerable to XSS. This field is protected against XSS strings and usernames larger than 20 characters, but with a proxy those defenses can be bypassed because they are triggered at client side.

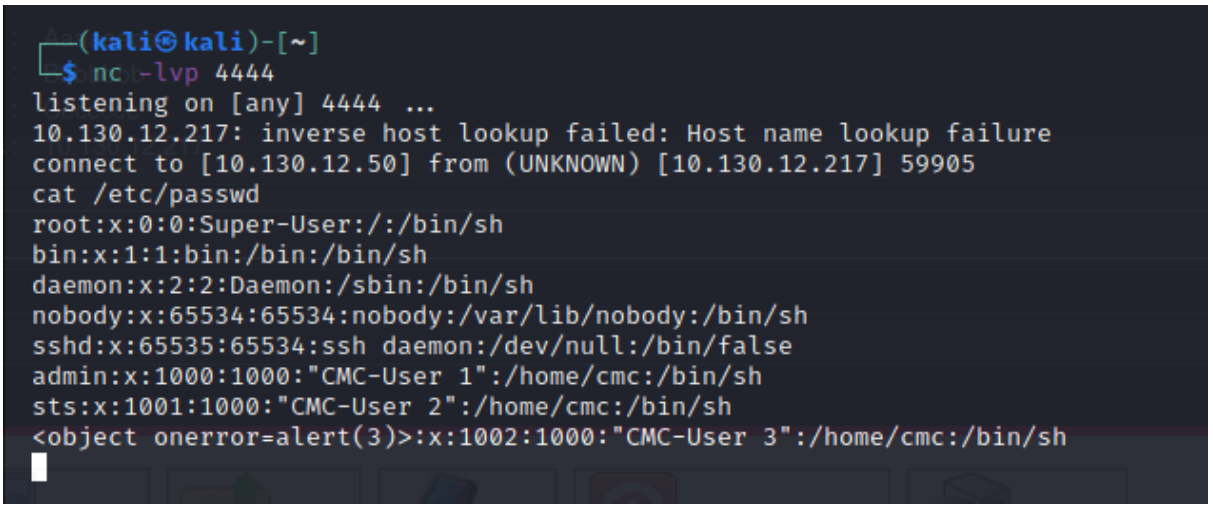
A possible payload that works is the following:

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

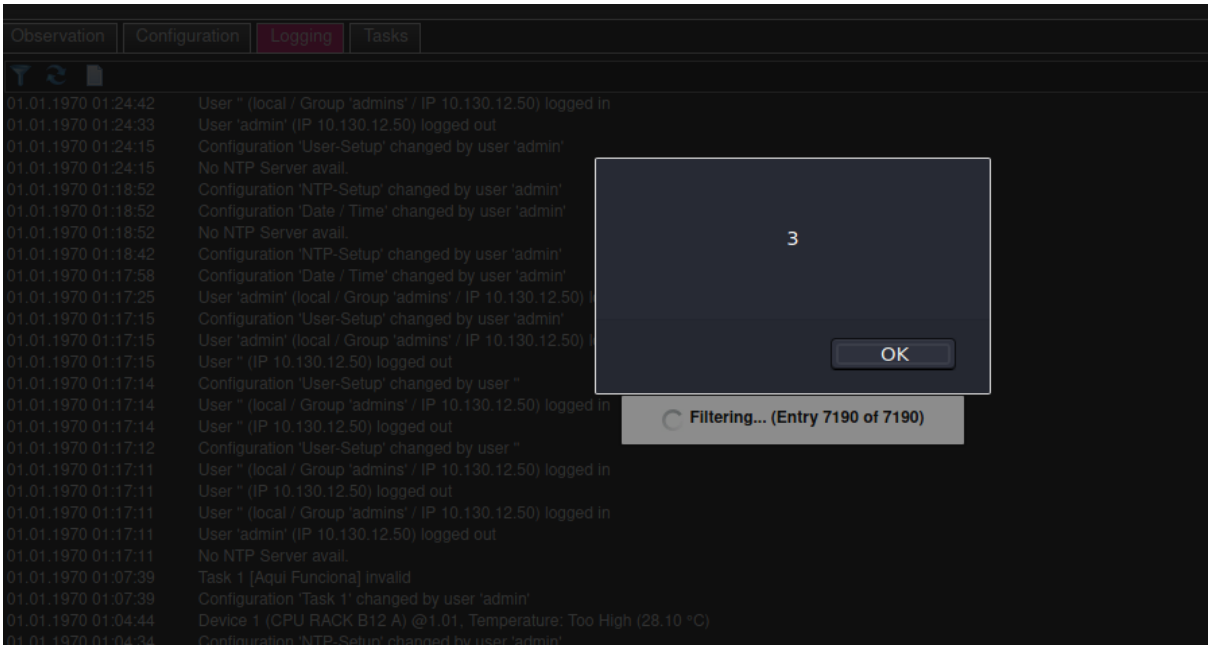
Once the user is created, we can login and the alert shows up.



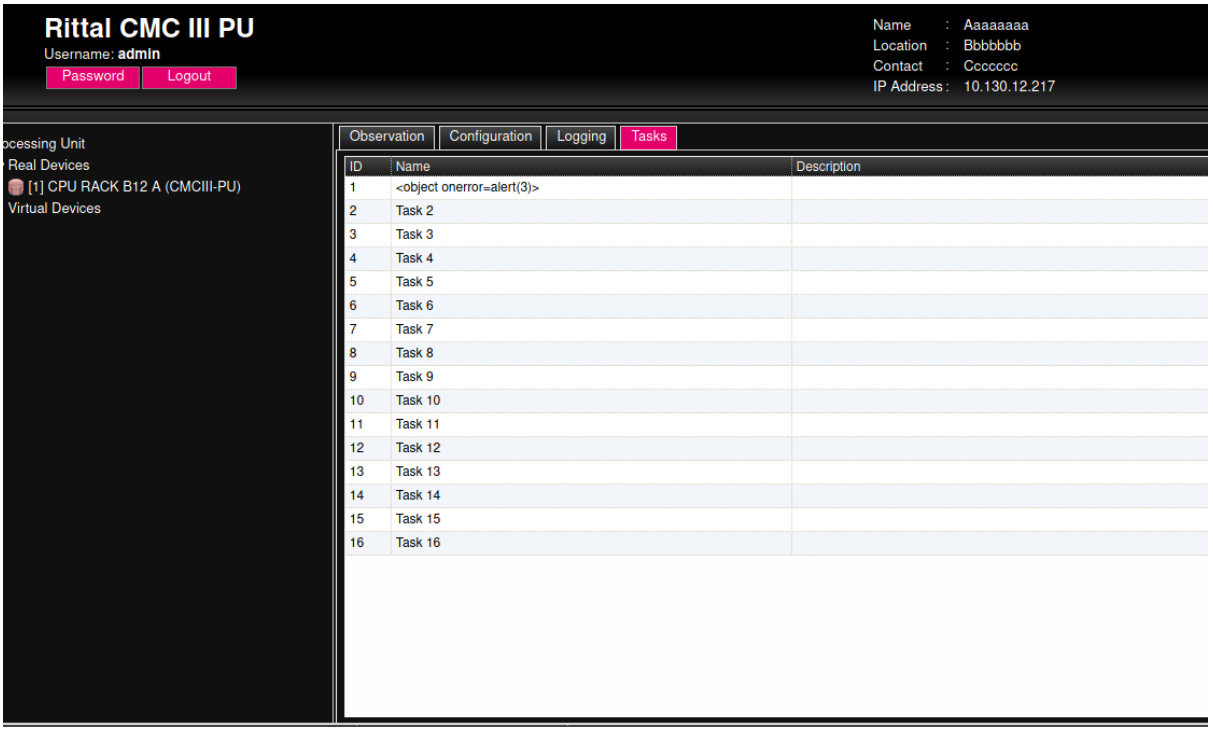
Note that the user is also created inside the device.



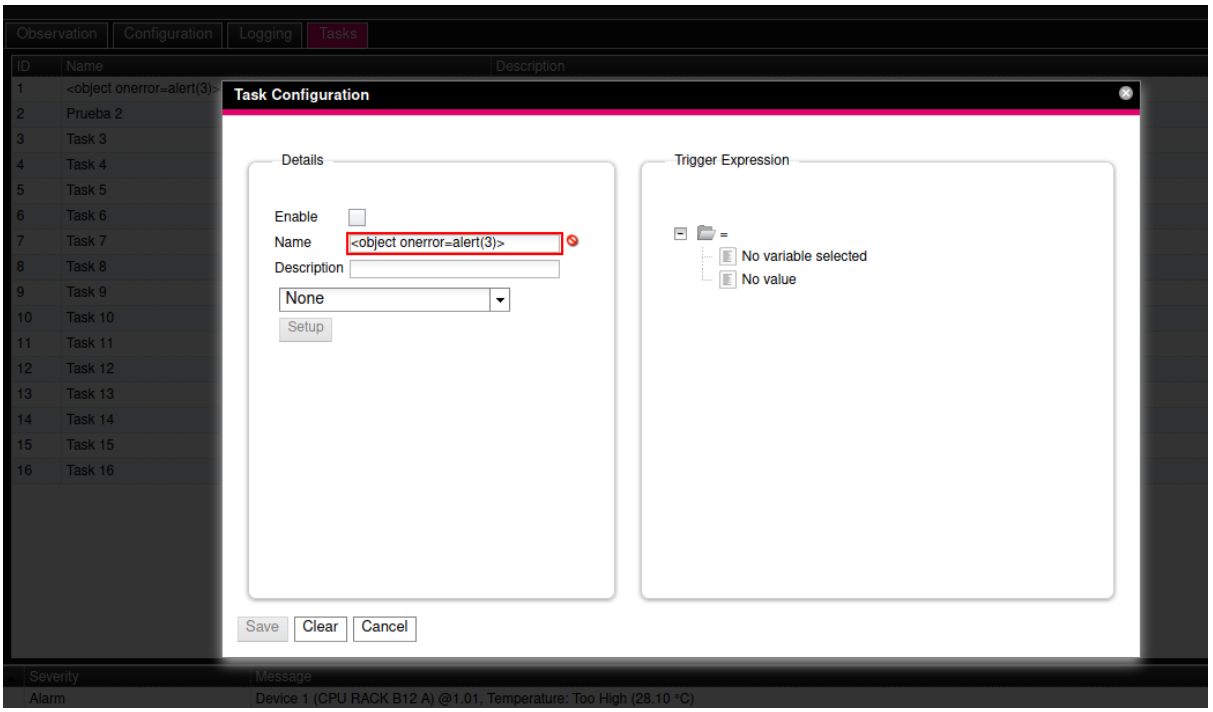
Everytime a user is logged, it creates a log that can be accessible in the Logging Tab. Here, the XSS is also stored. It will show up every time a user accesses the Loggin Tab until the logs are deleted.



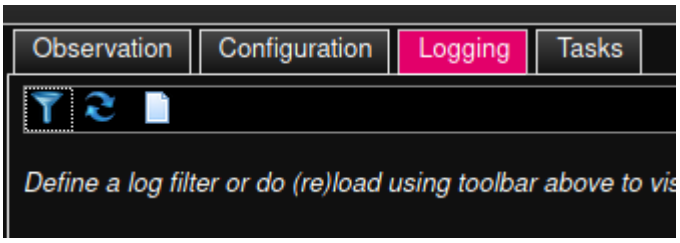
This stored XSS can also be created in the Task Tab, editing one task.

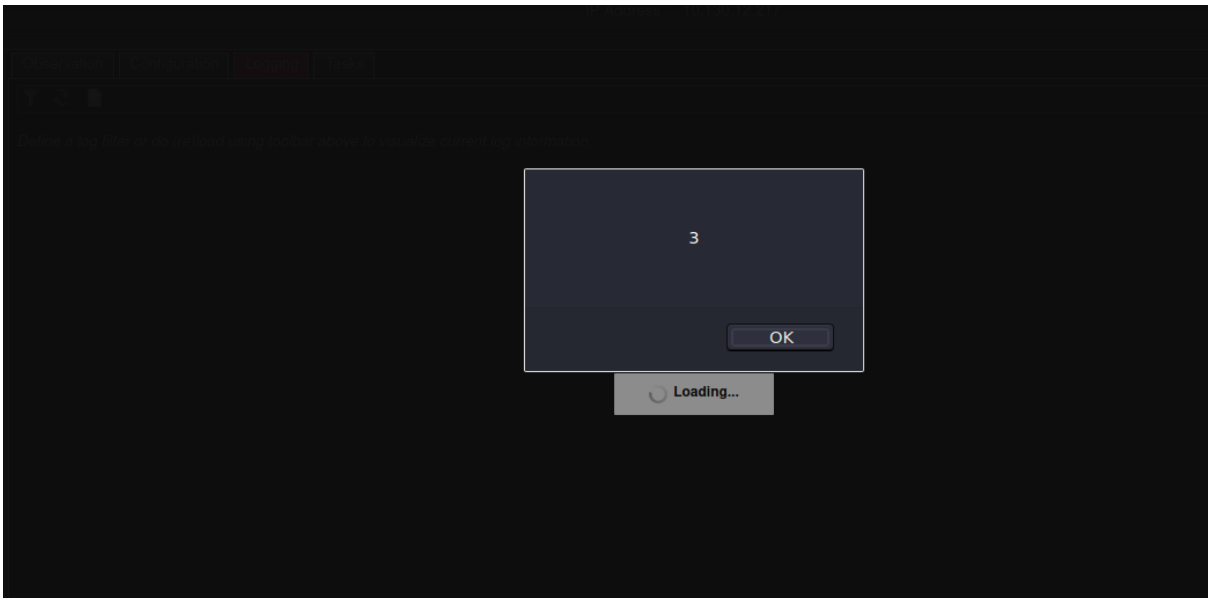


The procedure is the same, inserting the XSS with a proxy, as the sanitizing actions are done on client side.



Again, when accessing the Logging Tab 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 this attack.





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.