whitej3rry / **D-Link_DIR-605L_F1_CWE-1191.md** Secret

Created 3 months ago

Code Revisions 1

UART Root Shell Access on D-Link DIR-605L (Hardware F1, Firmware V6.02CN02)

D-Link_DIR-605L_F1_CWE-1191.md

CWE-1191: On-Chip Debug and Test Interface With Improper Access Control

UART Root Shell Access on D-Link DIR-605L (Hardware F1, Firmware V6.02CN02)

Summary

A critical hardware security vulnerability has been identified in the D-Link DIR-605L router, Hardware Version F1, Firmware External Version V6.02CN02, running Linux kernel 2.4.18. The UART debug interface lacks proper access control mechanisms, allowing any attacker with physical access to connect to the UART pins and gain unauthenticated root shell access. This vulnerability corresponds to CWE-1191: On-Chip Debug and Test Interface With Improper Access Control.

Affected Product:

Device Model: D-Link DIR-605L - Firmware Version: V6.02CN02

Vulnerability Description

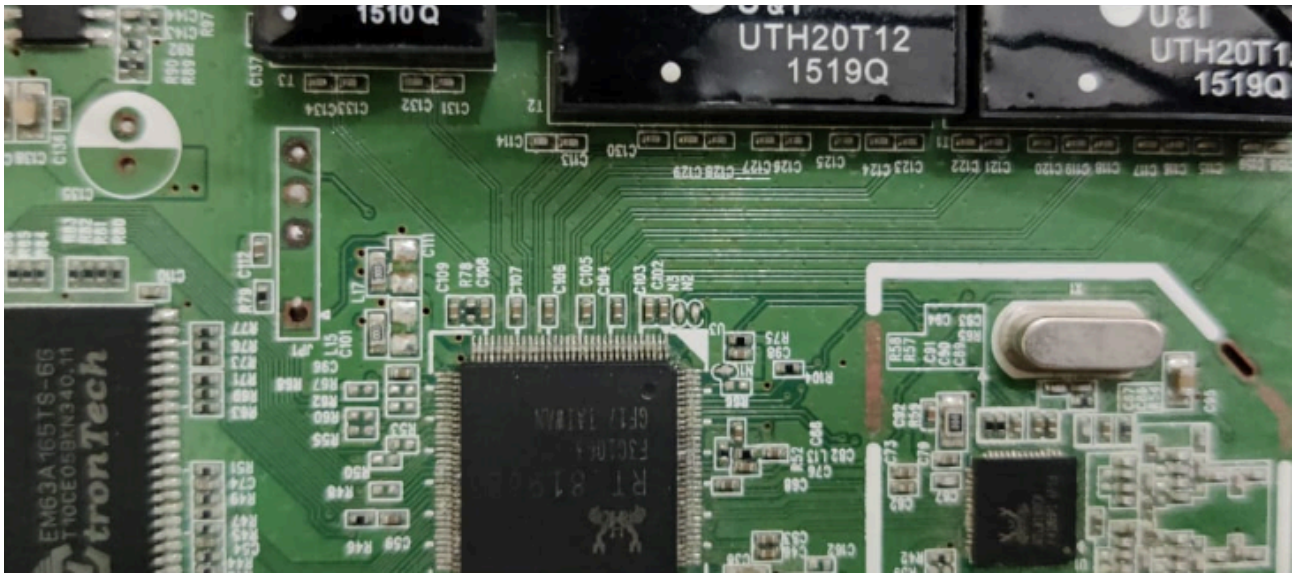
The UART debug interface, exposed physically via device pins, is accessible without any authentication or authorization barriers. An attacker connecting to these UART pins can instantly access the device's root shell during or after boot, bypassing all software-based authentication controls. This direct root shell access compromises the confidentiality, integrity, and availability of the entire device and its network environment.

Impact:

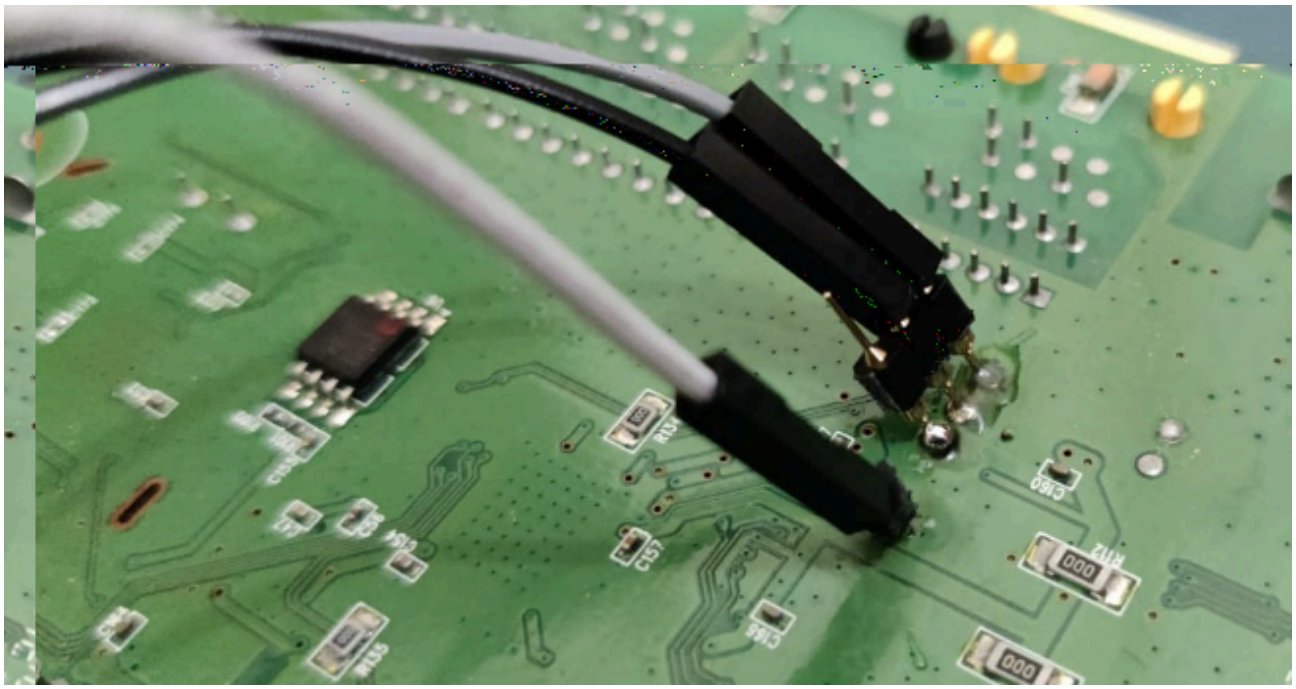
Full root-level control of the router with no authentication required. Ability to modify device configuration, install persistent malware, or intercept network traffic. Complete circumvention of on-device security mechanisms. Potential pivot point for attacks on the connected network and devices.

Proof of Concept:

1. The UART pins on the D-Link DIR-605L (Hardware F1) were identified and connected to a serial interface.



2. Using a serial terminal emulator at the appropriate baud rate, the device's bootloader output and Linux shell prompt were accessed.



3. Commands such as cat /etc/passwd confirmed root user presence without password protection on this interface.

```
# cat DevInfo.txt
Firmware External Version: 6.02CN02
Firmware Internal Version: f33e
Boot Code:
Model Name: DIR-605L
Hardware Version: F1
WLAN Domain: NA
Kernel: Linux version 2.4.18
Graphcal Authentication: Disable
WAN MAC:
LAN MAC:
WLAN MAC:
Language: English
# cat /etc/passwd
root:abSQTPcIskFGc:0:0:root:/:/bin/sh
nobody:x:99:99:Nobody:/:
```

4. A fully interactive root shell prompt (#) was obtained, enabling arbitrary command execution on the device.

```
boa: server version Boa/0.94.14rc21
boa: server built Mar  3 2015 at 14:20:28.
boa: starting server pid=20940, port 80
killall: mydlink-watch-dog.sh: no process killed
killall: signalc: no process killed
killall: tsa: no process killed
opt.local stop ok.
opt.local start ok.
20991
#
#
# cd /etc
# ls
```

References:

CWE-1191: https://cwe.mitre.org/data/definitions/1191.html

Author:

Mohamed Danish (j3rry)