BootIntel Security Report

Hardware Security Intelligence

TP-Link Archer C7 v5 (sample)

Scan ID: de094a88-9736-4efb-87fb-100000000000

Started: Jul 17, 2026 08:10:09 UTC

Completed: Jul 17, 2026 08:10:09 UTC

Exploit Score	8.6	Risk Level	CRITICAL

Executive Summary

3 critical findings identified. Prioritize the items below before shipping.

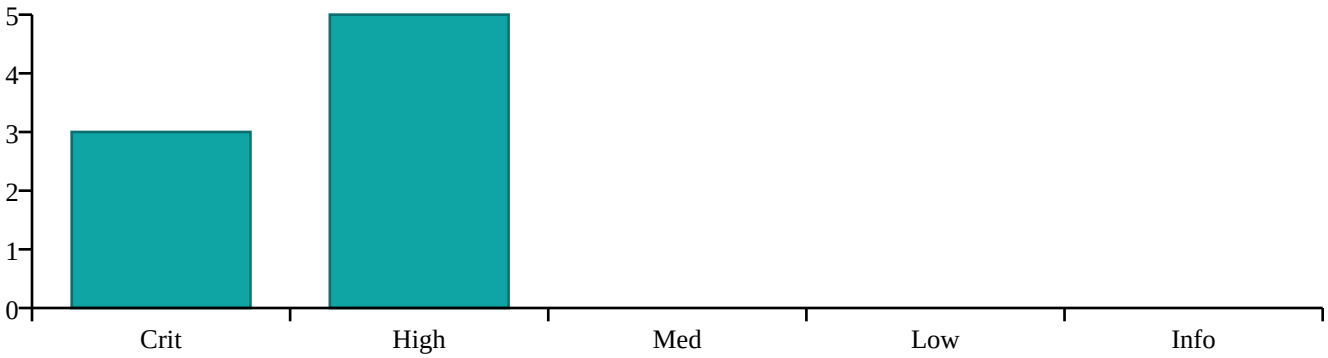
Top items to review:

1. [CRITICAL] CVE-2019-13103 — U-Boot 2019.01
Recommended: Update U-Boot to a patched version.

2. [CRITICAL] CVE-2019-14192 — U-Boot 2019.01
Recommended: Update U-Boot to a patched version.

3. [CRITICAL] Bootloader Interruption Possible
Recommended: Set bootdelay=-1 and enable U-Boot password protection (CONFIG_AUTOBOOT_KEYED).

Findings Distribution



Summary

Total Findings	Critical	High	Medium	Low	Info
8	3	5	0	0	0

System Overview

Bootloader	U-Boot 2019.01
Kernel	Linux 4.9.0
CPU	ARMv7 rev 5 (v7l). Cortex-A7
Architecture	ARM
RAM	256 MiB

Boot Fingerprint

Field	Value
Autoboot Delay	3
Autoboot Interruptible	True
Bootloader	U-Boot 2019.01
Bootloader Ver	2019.01
Kernel	Linux 4.9.0
Kernel Ver	4.9.0
Network Boot Activity	tftp/netboot
Userland	BusyBox 1.26.2

Hardware Details

Field	Value
Arch	ARM
Cpu	ARMv7 rev 5 (v7l). Cortex-A7
Dram	256 MiB

Software Inventory

Component	Version	Evidence
U-Boot	2019.01	—
Linux Kernel	4.9.0	—
BusyBox	1.26.2	—
uhttpd	detected	—

Attack Paths

Interrupt U-Boot Autoboot

• Connect UART adapter: TX->RX, RX->TX, GND->GND (3.3V logic).

• Open terminal at 115200.

• Power cycle and press key during autoboot countdown.

• Use U-Boot shell commands (for example, printenv).

CVE-2016-5195 - Dirty COW LPE

• Confirm vulnerable kernel version.

• Transfer/compile PoC.

• Execute exploit and verify root shell.

Induce U-Boot Fault to Trigger Shell Fallback

• Identify boot flash data line (NAND/SPI) and observe during kernel/ramdisk read.

• Introduce a short fault (pull data line low or glitch Vcc) to force a read failure.

• Watch UART for fallback behavior or a bootloader prompt.

• If shell appears, verify with 'printenv' and proceed cautiously.

Network Boot Image Hijack

• Identify boot server/protocol from logs.

• Position attacker on network path.

• Serve controlled boot artifacts.

Findings

Total Findings Included: 8

CVEs

Severity	CVE	Description	CVSS
CRITICAL	CVE-2019-13103	U-Boot 2019.01 is in the affected range for CVE-2019-13103 (CVSS 9.8). (L1)	9.8
CRITICAL	CVE-2019-14192	U-Boot 2019.01 is in the affected range for CVE-2019-14192 (CVSS 9.8). (L1)	9.8
HIGH	CVE-2016-5195	Linux Kernel 4.9.0 is in the affected range for CVE-2016-5195 (CVSS 7.8). (L8)	7.8
HIGH	CVE-2021-4034	Linux Kernel 4.9.0 is in the affected range for CVE-2021-4034 (CVSS 7.8). (L8)	7.8
HIGH	CVE-2022-28391	BusyBox 1.26.2 is in the affected range for CVE-2022-28391 (CVSS 8.8). (L13)	8.8

Other Findings

Severity	Finding	Evidence / Remediation
CRITICAL	Bootloader Interruption Possible	**Evidence:** Hit any key to stop autoboot: 3 **Remediation:** Set bootdelay=-1 and enable U-Boot password protection (CONFIG_AUTOBOOT_KEYED). Source: log line L6

Severity	Finding	Evidence / Remediation
HIGH	Telnet Daemon Running	**Evidence:** telnetd[1237]: listening on 0.0.0.0:23 **Remediation:** Disable telnetd and use SSH. Source: log line L17
HIGH	Network Boot Path Detected	**Evidence:** DHCP client bound to address 192.168.1.42 **Remediation:** Disable network boot for production or enforce authenticated image delivery. Source: log line L18