# CVE Detail – CVE-2020-10884

This vulnerability allows network-adjacent attackers execute arbitrary code on affected installations of TP-Link Archer A7 Firmware Ver: 190726 AC1750 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the tdpServer service, which listens on UDP port 20002 by default. This issue results from the use of hard-coded encryption key. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-9652.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.96358

## CVSS Scoring

CVSS v3.1 Score: 8.8

Severity: HIGH

## Mapped CWE(s)

* CWE-321: Use of Hard-coded Cryptographic Key
* CWE-798: Use of Hard-coded Credentials

## CAPEC(s)

* CAPEC-191: Read Sensitive Constants Within an Executable
* CAPEC-70: Try Common or Default Usernames and Passwords

## ATT&CK Techniques

* T1078.001: Default Accounts
* T1552.001: Credentials In Files

## Used By (Actors/Tools)

* TrickBot (malware)
* Stuxnet (malware)
* Smoke Loader (malware)
* HyperStack (malware)
* Emotet (malware)
* Hildegard (malware)
* BlackEnergy (malware)
* XTunnel (malware)
* pngdowner (malware)
* StrelaStealer (malware)
* Pysa (malware)
* Agent Tesla (malware)
* jRAT (malware)
* Azorult (malware)
* AADInternals (tool)
* Empire (tool)
* PoshC2 (tool)
* LaZagne (tool)
* Pupy (tool)
* QuasarRAT (tool)
* Indrik Spider (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* TA505 (intrusion-set)
* Ember Bear (intrusion-set)
* TeamTNT (intrusion-set)
* Leafminer (intrusion-set)
* Magic Hound (intrusion-set)
* MuddyWater (intrusion-set)
* Kimsuky (intrusion-set)
* FIN13 (intrusion-set)
* Scattered Spider (intrusion-set)
* RedCurl (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* APT3 (intrusion-set)
* HomeLand Justice (campaign)
* APT33 (intrusion-set)

## Affected Products

* cpe:2.3:o:tp-link:ac1750\_firmware:190726:\*:\*:\*:\*:\*:\*:\*