Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

TP-Link Router End-of-Service Models Exploited in Botnet Operation

Date of Publication	Admiralty Code	TA Number
September 5, 2025	A1	TA2025270

Summary

Affected Products: TP-Link Multiple Routers
Threat Actor: Storm-0940
Malware: Quad 7 (7777) Botnet (aka CovertNetwork-1658, xlogin)
Impact: Two critical TP-Link router flaws (CVE-2023-50224 and CVE-2025-9377) have been exploited by the Quad7 botnet to steal credentials and execute malicious code, thereby fueling large-scale password spray and brute-force attacks on Microsoft 365 accounts. Quad7 has been linked to Chinese threat actors, such as Storm-0940, who reuse stolen credentials for global intrusions. While TP-Link has released patches, only routers with remote administration exposed to the internet are at risk, making secure configurations and timely updates essential.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-50224	TP-Link TL-WR841N Authentication Bypass by Spoofing Vulnerability	TP-Link TL-WR841N	✗	✓	✓
CVE-2025-9377	TP-Link Archer C7(EU) and TL-WR841N/ND(MS) OS Command Injection Vulnerability	TP-Link Multiple Routers	✗	✓	✓

Vulnerability Details

#1 Two critical security flaws have been discovered in TP-Link wireless routers, tracked as CVE-2023-50224 and CVE-2025-9377. CVE-2023-50224 enables attackers to steal stored router passwords. CVE-2025-9377 is a command injection vulnerability in the Parental Control feature, which allows for remote code execution (RCE).

#2 Since August 2023, adversaries have carried out highly evasive password spray attacks that successfully stole credentials from multiple Microsoft customers. These attacks originated from a network of compromised devices forming the Quad7 (7777) botnet, also referred to as CovertNetwork-1658 or xlogin.

#3 The Quad7 botnet is associated with devices that expose TCP port 7777 and display a "xlogin:" banner. The botnet deployed Socks5 proxies on compromised devices, which are then used to relay slow brute-force attempts against Microsoft 365 accounts worldwide. One affected model that was monitored, the TP-Link WR841N (3.16.9 Build 150320 Rel.57500n), is particularly vulnerable to the chained exploit leveraged by the Quad7 botnet.

#4 Multiple Chinese threat actors reuse credentials stolen through these password spray operations. Among them, Storm-0940, which has been active since at least 2021, uses Quad7-acquired credentials. This actor typically gains initial access through password spraying, brute-force attacks, or exploitation of internet-facing applications and services.

#5 A notable attack chain combined two flaws. First, an unauthenticated file disclosure allowed the retrieval of credentials stored in /tmp/dropbear/dropbearpwd. These were then replayed against the management interface using HTTP Basic authentication (CVE-2023-50224). Once authenticated, the attacker exploited the command injection vulnerability in the Parental Control page by tampering with the url_0 parameter to achieve RCE (CVE-2025-9377).

#6 Although the router models exploited by Quad7 are already past their End of Service (EOS) date, TP-Link has released firmware updates addressing these vulnerabilities. Importantly, this exploit chain only functions if the router's remote administration interface is exposed to the internet, which is disabled by default in TP-Link firmware.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-50224	TP-Link TL-WR841N routers	cpe:2.3:o:tp-link:tl-wr841n_firmware:3.16.9:build_200409:*:*:*:*:*:*:* cpe:2.3:h:tp-link:tl-wr841n:12:*:*:*:*:*:*:*	CWE-290
CVE-2025-9377	Archer C7(EU) V2: before 241108 and TL-WR841N/ND(MS) V9: before 241108	cpe:2.3:o:tp-link:tl-wr841n_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:tp-link:tl-wr841n:v9:*:*:*:*:*:*:* cpe:2.3:o:tp-link:tl-wr841nd_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:tp-link:tl-wr841nd:9:*:*:*:*:*:*:* cpe:2.3:o:tp-link:archer_c7_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:tp-link:archer_c7:2.0:*:*:*:*:*:*:*	CWE-78

Recommendations

Immediate Firmware Updates: Users of TP-Link TL-WR841N/ND (MS) V9 (Firmware: 3.16.9 Build 150320 Rel.57500n) and Archer C7 (EU) V2 (Firmware: 3.15.3 Build 180305 Rel.51282n) should immediately apply the latest patched firmware: Archer C7(EU) V2 Firmware, TL-WR841N(MS) V9 Firmware, TL-WR841ND(MS) V9 Firmware. Ensure firmware is downloaded only from the official TP-Link website corresponding to your purchase region. Verify the hardware version before upgrading. Installing the wrong firmware may permanently damage the device and void the warranty.

Router Configuration Hardening: Disable Remote Management unless necessary, manage routers locally or through the TP-Link Tether App. Reboot and restore the router after patching to ensure secure and stable management access. Regularly review and update admin passwords, avoiding reuse of credentials across different services.

Safe Firmware Upgrade Practices: Use a wired connection when upgrading to prevent disconnections. Do not power off the router during the upgrade process. Stop all internet applications or disconnect the WAN cable during the upgrade. Extract the downloaded firmware file using tools like WinRAR/WinZIP before applying it.

Replacement of End-of-Life Devices: Both the TL-WR841N/ND V9 and Archer C7 V2 are End-of-Life (EOL) and will not receive ongoing security support. For stronger security and performance, upgrade to newer TP-Link router families with enhanced hardware security models. If an EOL router is still under warranty, TP-Link may provide an equivalent or upgraded replacement based on availability.

Security Best Practices: Regularly check TP-Link's firmware update page and EOL notices for affected products. Segment IoT and critical business devices onto separate networks to reduce risk exposure. Monitor for unusual traffic patterns, which may indicate botnet involvement. Implement strong account security for Microsoft 365 and other services targeted by password spray attacks enable MFA wherever possible.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0011** Command and Control	**TA0040** Impact
T1078 Valid Accounts	**T1110** Brute Force	**T1110.003** Password Spraying	**T1190** Exploit Public-Facing Application
T1203 Exploitation for Client Execution	**T1059** Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1552** Unsecured Credentials

T1552.001 Credentials In Files	**T1110** Brute Force	**T1087** Account Discovery	**T1046** Network Service Discovery
T1090 Proxy	**T1090.003** Multi-hop Proxy	**T1071.001** Web Protocols	**T1071** Application Layer Protocol
T1571 Non-Standard Port	**T1496** Resource Hijacking		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	142[.]11[.]205[.]164, 23[.]254[.]201[.]175, 151[.]236[.]20[.]185, 151[.]236[.]20[.]211
IPv4:Port	158[.]247[.]194[.]125[:]80, 45[.]77[.]44[.]119[:]80, 151[.]236[.]20[.]30[:]80, 103[.]140[.]239[.]63[:]80, 103[.]57[.]248[.]202[:]81
MD5	98d3764862b182417c910a96e0fbfe71, c8e229bed1659f1613c1016b3345ef08, 29e6df5bb30ed8fd12c09d9b6890ab4f, 69ced04a2ec895084d3aab1086216d32, 408152285671bbd0e6e63bd71d6abaaf, 5efc7d824851be9ec90a97d889a40d23, f42849076e24b7827218f7a25bc11ccc, 92093dd7ba6ae8fe34a215c4c4bd1cd4, e6f6a6de285d7c2361c32b1f29a6c3f6, b3b09819f820a4ecd31f82f369000af2, 3c4b3d1480952d6ddfe434fef07054f7, cdb37db4543dde5ca2bd98a43699828f, 22633ef920f0093e3d720e7bbeb9fec8, d617f43163cb0f355dbf63058aa82d1d, 150d444848a02be230ed9fbf3692d226, 43ea387b8294cc4d0baaef6d26ff7c72, 4d9067e7cf517158337123a30a9bd0e3, 8542a3cbe232fe78baa0882736c61926, 777d6f907da38365924a0c2a12e973c5,

TYPE	VALUE
MD5	470c6ee61b4314721a8cc9ebafe8fef8, 1b08725acc371f6b7d05bb72d0c2d759, 40b5ac87ff87634c48fdd2cf64ccb66b, 199045538d9c139f9cf562d5b76a5cd5, 4b8e97260d9ef6ca774675be682d9c8c, 5b0a28631ca106c31e1d5e81d8e25297

Patch Links

CVE-2023-50224:
https://www.tp-link.com/en/support/download/tl-wr841n/v12/#Firmware

CVE-2025-9377:
https://www.tp-link.com/us/support/faq/4308/

References

https://www.tp-link.com/us/support/faq/4365/

https://www.cisa.gov/news-events/alerts/2025/09/03/cisa-adds-two-known-exploited-vulnerabilities-catalog

https://blog.sekoia.io/solving-the-7777-botnet-enigma-a-cybersecurity-quest/

https://blog.sekoia.io/a-glimpse-into-the-quad7-operators-next-moves-and-associated-botnets/

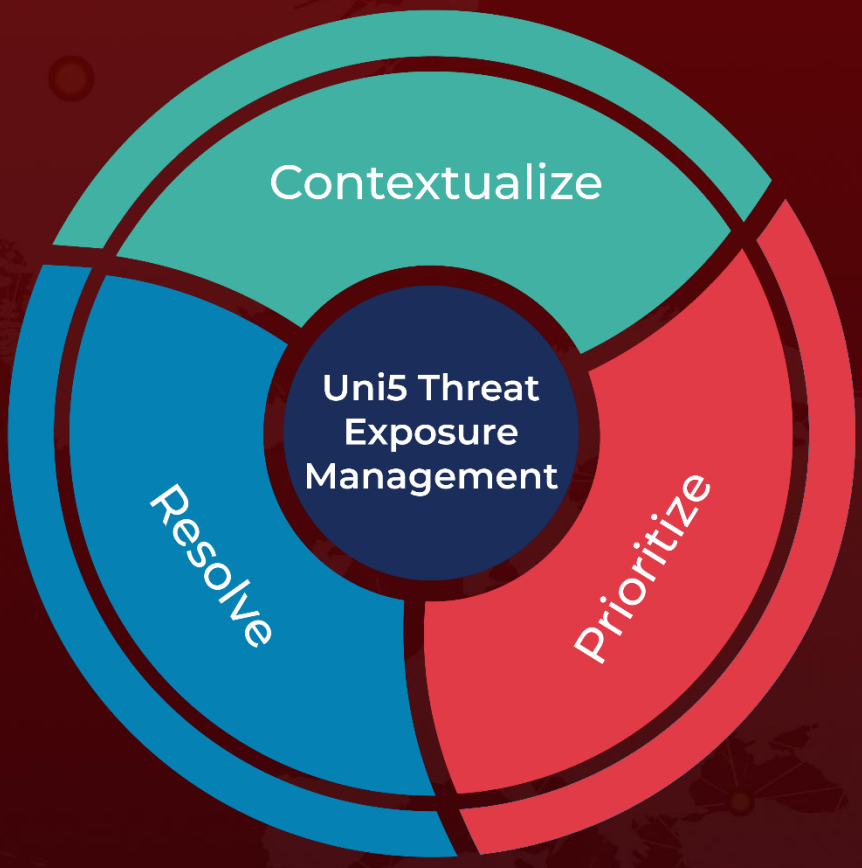
https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/

https://www.tp-link.com/nordic/support/faq/3562/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 5, 2025 . 6:30 AM

More at www.hivepro.com