# CVE-2020-24363

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-24363 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-08-31 16:15:00 UTC |
| **Updated** | 2020-09-08 17:41:00 UTC |
| **Description** | TP-Link TL-WA855RE V5 20200415-rel37464 devices allow an unauthenticated attacker (on the same network) to submit a |

## Risk And Classification

**EPSS:** 0.126120000 probability, percentile 0.940340000 (date 2026-05-14)

**CISA KEV:** Listed on 2025-09-02; due 2025-09-23; ransomware use Unknown

**Problem Types:** CWE-306

## CISA Known Exploited Vulnerability

| | |
|---|---|
| **Vendor** | TP-Link |
| **Product** | TL-WA855RE |
| **Name** | TP-link TL-WA855RE Missing Authentication for Critical Function Vulnerability |
| **Required Action** | Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. |
| **Notes** | https://www.tp-link.com/us/home-networking/range-extender/tl-wa855re/#overview ; https://www.tp-link.com/us/support/download/tl-wa855re/#FAQs ; https://nvd.nist.gov/vuln/detail/CVE-2020-24363 |

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Hardware | Tp-link | Tl-wa855re | v5 | All | All | All |
| Hardware | Tp-link | Tl-wa855re | v5 | All | All | All |
| Operating System | Tp-link | Tl-wa855re Firmware | 20200415 | All | All | All |
| Operating System | Tp-link | Tl-wa855re Firmware | 20200415 | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|

| | | | |
|---|---|---|---|
| CVE-2020-24363 TL-WA855RE V5 advisory – malwrforensics | MISC | malwrforensics.com | Third Party Advisory |
| Download for TL-WA855RE \| TP-Link | MISC | www.tp-link.com | Vendor Advisory |
| CVE-2020-24363 - Pastebin.com | MISC | pastebin.com | Third Party Advisory |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |
| CISA Known Exploited Vulnerabilities catalog | CISA | www.cisa.gov | kev |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status** **status.cve.report**