INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-02 06:32 UTC

CVE-2026-10119: A security vulnerability has been detected in TRENDnet TEW-432BRP 3.10B20. Impacted is the function ...

CVE VULNERABILITY | HIGH | CVSS 8.8

SCC Item ID	SCC-CVE-2026-0251
Type	CVE Vulnerability
CVE ID	CVE-2026-10119
Severity	HIGH
CVSS Base Score	8.8
EPSS Score	0.0004 (13th percentile)
Affected Products	TRENDnet TEW-432BRP firmware version 3.10B20
Published	2026-05-30T14:16:24.513
Discovery Source	Nvd

Executive Summary

A stack-based buffer overflow vulnerability (CVE-2026-10119, CVSS 8.8) affects the TRENDnet TEW-432BRP router running firmware 3.10B20. The device, released circa 2009, has long exceeded typical vendor support lifecycles, and TRENDnet has confirmed no patch will be issued, leaving any organization still operating this hardware permanently exposed. The primary business risk is network compromise through an internet-facing or insufficiently isolated legacy device that cannot be remediated through software updates.

Technical Analysis

CVE-2026-10119 is a stack-based buffer overflow (CWE-121, CWE-119) in the formSetMACFilter function, reachable via HTTP POST to /goform/formSetMACFilter on TRENDnet TEW-432BRP routers running firmware 3.10B20. The vulnerability is triggered by supplying an oversized filter_name argument, overwriting stack memory and enabling arbitrary code execution. Attack vector is network-based; authentication requirements have not been confirmed as mandatory in public disclosures reviewed. A public exploit has been reportedly disclosed in security community forums. MITRE ATT&CK maps this to T1190 (Exploit Public-Facing Application). CVSS 8.8 is sourced from NVD; vector string is pending full NVD publication. No patch exists and none will be issued. The EPSS score is 0.041% (12.8th percentile), indicating currently low observed

exploitation activity, but the public exploit disclosure increases that risk over time. CISA KEV listing: not present as of configuration date.

Action Checklist

1. Step 1: Containment, Identify all TRENDnet TEW-432BRP devices running firmware 3.10B20 in your environment using asset inventory tools (aligned with CIS 1.1 best practices). Immediately block inbound and outbound internet access to these devices at the perimeter firewall. If the device is internal-only, isolate it to a dedicated VLAN with no cross-segment routing until it can be decommissioned.
2. Step 2: Detection, Query network flow logs and firewall logs for HTTP POST requests targeting the URI /goform/formSetMACFilter on the management IP of any TEW-432BRP device. Look for oversized or malformed filter_name parameter values in web server logs on the device, if accessible. If the device supports syslog or web log export, query for crash events or unexpected reboots. Check for unexpected outbound connections from the device IP that would indicate post-exploitation callback activity (NIST AU-6, AU-12).
3. Step 3: Eradication, No vendor patch exists and none will be issued. The only full eradication path is hardware decommission and replacement with a supported device. Remove the TEW-432BRP from production and substitute a currently supported router model. Document removal per asset inventory process (CIS 1.1, CIS 2.2, ensure authorized software/hardware is currently supported).
4. Step 4: Recovery, After replacing the device, validate that no lateral movement occurred from the affected router to adjacent network segments by reviewing authentication logs (NIST AU-6) and checking for unauthorized account creation (NIST AC-2, CIS 5.1). Confirm replacement device is configured to baseline (CIS 4.2) and management interface is not internet-exposed. Monitor replacement device logs for 30 days post-cutover.
5. Step 5: Post-Incident, This exposure indicates a gap in asset lifecycle management. Audit the full network inventory for additional end-of-life devices with no vendor support path (CIS 1.1, CIS 2.2). Establish a formal EOL tracking process tied to vulnerability management (CIS 7.1). Review firewall rules to confirm management interfaces on all network devices are not reachable from untrusted networks (NIST AC-17, CIS 4.4).

Detection Guidance

Query perimeter and internal firewall logs for HTTP POST traffic directed to /goform/formSetMACFilter on the management IP(s) of any TEW-432BRP device. Flag requests with abnormally large filter_name field values (exceeding typical MAC filter name length of 32 characters). If the device management interface is accessible via SIEM log forwarding or syslog, look for crash events or unexpected reboots, which may indicate failed or successful exploitation attempts. Post-exploitation indicators include unexpected outbound TCP connections from the device IP to external addresses, DNS queries from the device IP to non-configured resolvers, or ARP table anomalies suggesting traffic redirection. No confirmed IOCs have been published in the sources reviewed; behavioral detection is the primary available method. Reference NIST SI-4 for system monitoring requirements and AU-6 for audit review cadence.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation
- **SI-4** — System Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **8.2** — Collect Audit Logs

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-10119	T1

Source	URL	Tier
CVE-2026-5119 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2026-5119	T3
CVE-2026-10119 Affects TRENDnet TEW-432BRP Router : r/pwnhub	https://www.reddit.com/r/pwnhub/comments/1tsw2lo/critical_security_...	T3
CVE-2026-1919: WordPress Booktics Auth Bypass Vulnerability	https://www.sentinelone.com/vulnerability-database/cve-2026-1919/	T3
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1

Generated 2026-06-02 06:32 UTC by TJS Security Command Center