INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-23 06:38 UTC

Mirai 'tuxnokill' Botnet Actively Exploits Unpatched RCE in EoL D-Link DIR-823X Routers

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0206
Type	Threat Campaign
CVE ID	CVE-2025-29635, CVE-2023-1389
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0125 (79th percentile)
Affected Products	D-Link DIR-823X routers (firmware 240126 and 240820, EoL November 2024); TP-Link routers (CVE-2023-1389); ZTE ZXV10 H108L routers
Published	2026-04-22T16:04:46
Discovery Source	Rss

Executive Summary

A Mirai botnet variant called 'tuxnokill' is actively exploiting a remote code execution vulnerability in D-Link DIR-823X routers, confirmed by Akamai SIRT via honeypot telemetry in March 2026. These routers reached end-of-life in November 2024, meaning no vendor patch will ever be issued, and any exposed device is permanently vulnerable at the firmware level. Organizations or managed service providers still running these devices on internet-facing networks face immediate risk of device compromise and recruitment into DDoS infrastructure.

Technical Analysis

Akamai SIRT confirmed active in-the-wild exploitation of CVE-2025-29635 (CWE-77, CWE-78: command injection) affecting D-Link DIR-823X routers on firmware versions 240126 and 240820. Exploitation enables unauthenticated remote code execution via a command-injection attack path consistent with Mirai-variant initial access techniques (MITRE T1190). Post-exploitation activity includes payload delivery (T1105), shell execution (T1059, T1059.004), and device enrollment into DDoS botnet infrastructure (T1498, T1498.001). The campaign also leverages CVE-2023-1389, a previously documented TP-Link command injection flaw (CVSS 9.8 per NVD), used by multiple prior Mirai variants, and targets ZTE ZXV10 H108L devices. CVE-2025-29635 carries a CVSS base score of 7.5 and sits at the 79th EPSS percentile (score: 0.0125), indicating elevated exploitation probability relative to the broader CVE population. No vendor patch exists or will be issued for the D-Link device;

end-of-life was declared November 2024. Mitigation requires hardware replacement or strict network isolation. Infrastructure acquisition techniques (T1583.003, T1583.005) suggest the operator is actively building botnet capacity.

Action Checklist

1. Containment: Immediately identify all D-Link DIR-823X routers (firmware 240126 or 240820), TP-Link routers vulnerable to CVE-2023-1389, and ZTE ZXV10 H108L devices in your inventory. Block inbound management traffic (HTTP/HTTPS/Telnet) to these devices at the perimeter firewall. If the device is internet-facing, isolate it from the network immediately pending replacement.
2. Detection: Query firewall and NetFlow logs for outbound connections from router management IPs to uncommon external destinations, particularly high-volume UDP flows indicative of DDoS participation. Review DHCP and ARP tables for unexpected device behavior. Check for Mirai-variant indicators: Telnet brute-force attempts, wget/curl fetches from unknown external IPs, and unexpected process spawning. Cross-reference source IPs against Akamai SIRT's published IOCs for the tuxnokill campaign.
3. Eradication: No firmware patch is available or forthcoming for the D-Link DIR-823X; remediation requires physical hardware replacement with a supported device. For TP-Link devices, apply the vendor-issued patch for CVE-2023-1389 per TP-Link's official advisory. For ZTE ZXV10 H108L, contact ZTE support for current firmware guidance. Do not return any unpatched or EoL device to internet-facing service.
4. Recovery: After replacing affected hardware, verify new devices run current, supported firmware from the vendor's official download page. Confirm no lateral movement occurred from compromised routers to internal hosts by reviewing authentication logs and DNS query history for the period of potential exposure. Re-scan the network segment for any residual Mirai-variant indicators before restoring normal traffic flows.
5. Post-Incident: Conduct an asset inventory audit to identify any additional end-of-life network devices still in production. Establish a lifecycle management policy requiring vendor support status verification before deployment and a defined replacement schedule for devices approaching EoL. Map this gap to CIS Control 1 (Inventory and Control of Enterprise Assets) and NIST CSF Identify function. Document the 13-month gap between initial CVE disclosure and active exploitation as a data point for patch prioritization SLA review.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal, and executive stakeholders immediately if: (1) evidence of tuxnokill DDoS participation is confirmed from your network (outbound volumetric UDP/TCP flood traffic), which may trigger upstream provider abuse notifications or regulatory scrutiny; (2) lateral movement from the compromised DIR-823X to internal hosts processing PII, PHI, or PCI-DSS cardholder data is detected, triggering breach notification obligations; or (3) your organization lacks the internal capability to replace all identified EoL devices within 24 hours, requiring managed service provider or emergency procurement escalation.

Recovery Notes	After replacing DIR-823X hardware and patching TP-Link devices, monitor outbound traffic from the replacement devices and adjacent network segment for a minimum of 14 days using NetFlow or firewall logging, specifically watching for any resumption of high-volume UDP flows or outbound Telnet connections that would indicate a Mirai re-infection from a missed device or a previously infected internal host acting as a secondary propagation vector. Validate that no internal hosts acquired tuxnokill binaries during the exposure window by running a filesystem scan using ClamAV with an updated Mirai signature database ('freshclam && clamscan -r /tmp /var/tmp /dev/shm') on any Linux-based internal systems that communicated through the compromised router. Retain enhanced logging posture on all network edge devices for 30 days post-recovery to detect any re-targeting by the tuxnokill campaign infrastructure.
Forensic Artifacts	Router /tmp and /var/run filesystem contents (via console access before decommission): tuxnokill Mirai variants drop their malware binary as a randomly-named ELF executable in /tmp or /dev/shm on the DIR-823X embedded Linux filesystem — capture 'ls -la /tmp /dev/shm /var/run' output and binary hashes as primary malware evidence | Firewall and NetFlow logs showing outbound connections from DIR-823X WAN IP: look for high-volume UDP flows on ports 7547 (TR-069), 5555 (ADB), and random high ports characteristic of Mirai DDoS attack modules, plus outbound TCP/23 Telnet scan sweeps indicating botnet propagation attempts to adjacent devices | Web server / reverse proxy access logs for the DIR-823X management interface: CVE-2025-29635 is an RCE exploited via the router's HTTP management interface — capture and preserve any access logs showing POST requests to CGI endpoints (e.g., '/cgi-bin/') with anomalous payloads containing shell command injection strings (semicolons, pipe characters, backtick-encoded commands) from external source IPs | DNS resolver query logs for the exposure window: Mirai tuxnokill variant C2 communication and binary download (via wget/curl as noted by Akamai SIRT) will generate DNS queries from the router's IP — preserve resolver logs showing domains queried by the router IP, particularly any that resolved to IPs matching Akamai SIRT's published tuxnokill C2 infrastructure IOCs | ARP and MAC address table snapshots from upstream switch/router at time of isolation: documents all devices that were in active communication with the compromised DIR-823X at the moment of containment, establishing the full blast radius for lateral movement analysis and providing a device list for follow-on scanning

Per-Action IR Details

Containment — Immediately identify all D-Link DIR-823X routers (firmware 240126 or 240820), TP-Link routers vulnerable to CVE-2023-1389, and ZTE ZXV10 H108L devices in your inventory. Block inbound management traffic (HTTP/HTTPS/Telnet) to these devices at the perimeter firewall. If the device is internet-facing, isolate it from the network immediately pending replacement.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST SC-7 (Boundary Protection), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run 'nmap -p 23,80,443,8080 --open ' to enumerate devices with Telnet/HTTP exposed; cross-reference MAC OUI prefixes (D-Link OUI: 1C:7E:E5, B0:C5:54, etc.) against ARP table output ('arp -a' on Windows or 'ip neigh' on Linux) to locate all DIR-823X devices without a full CMDB. Apply perimeter ACL blocking TCP/23, TCP/80, TCP/443, TCP/8080 inbound to identified management IPs using iptables or firewall CLI immediately. Isolate suspected compromised devices by placing their switchport into a quarantine VLAN ('switchport access vlan ' on Cisco IOS) pending physical replacement.

Evidence: Before isolating, capture a full NetFlow or sFlow export from the upstream router/switch covering the DIR-823X management IP for the prior 72 hours — specifically flag any outbound TCP/23 (Telnet) sessions to external IPs, which would indicate tuxnokill's Telnet-based propagation. Export current ARP and MAC address tables ('show arp' and 'show mac address-table' on Cisco) to document what hosts the compromised router was communicating with. Capture the router's current running configuration via console if accessible, as tuxnokill may have injected a persistent cron job or modified /etc/init.d startup scripts on the embedded Linux firmware.

Detection — Query firewall and NetFlow logs for outbound connections from router management IPs to uncommon external destinations, particularly high-volume UDP flows indicative of DDoS participation. Review DHCP and ARP tables for unexpected device behavior. Check for Mirai-variant indicators: Telnet brute-force attempts, wget/curl fetches from unknown external IPs, and unexpected process spawning. Cross-reference source IPs against Akamai SIRT's published IOCs for the tuxnokill campaign.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM, query firewall logs directly using grep or awk: 'grep -E "(src=)" /var/log/firewall.log | awk '{print $dst}' | sort | uniq -c | sort -rn' to surface high-frequency outbound destinations. For DDoS participation detection, run 'tcpdump -i -nn src and udp' on an upstream Linux host to capture volumetric UDP flood traffic characteristic of Mirai DDoS commands (SYN flood, UDP flood, ACK flood). Use Wireshark with display filter 'ip.src == && tcp.dstport == 23' to identify outbound Telnet brute-force propagation attempts targeting other devices. Deploy the Akamai SIRT's published tuxnokill YARA rules (when released) via standalone YARA scan on any captured pcap files. Use ntopng (free tier) for real-time flow analysis if tcpdump is not viable.

Evidence: Pull firewall deny/allow logs for the DIR-823X WAN IP and search for HTTP POST requests to URI paths consistent with CVE-2025-29635 exploitation (the RCE likely targets a specific CGI endpoint in the DIR-823X web management interface — look for anomalous POST requests with shell metacharacters or encoded payloads in the URI or body). Check upstream DNS resolver logs for queries from the router's IP to domains associated with Mirai C2 infrastructure (random-looking domains or direct IP-based C2 — Mirai variants historically avoid DNS for C2 but use it for NTP and update fetches). Capture any wget/curl command strings in router syslog output (if syslog forwarding was enabled to a remote server) which would show the tuxnokill binary download URL and C2 IP.

Eradication — No firmware patch is available or forthcoming for the D-Link DIR-823X; remediation requires physical hardware replacement with a supported device. For TP-Link devices, apply the vendor-issued patch for CVE-2023-1389 per TP-Link's official advisory. For ZTE ZXV10 H108L, contact ZTE support for current firmware guidance. Do not return any unpatched or EoL device to internet-facing service.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), NIST SA-22 (Unsupported System Components), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For TP-Link CVE-2023-1389 patching: download firmware exclusively from TP-Link's official support portal (tp-link.com/en/support/download/), verify the SHA-256 checksum of the firmware binary against the value published in the official advisory before flashing — do not source firmware from third-party mirrors. For ZTE ZXV10 H108L: open a support ticket with ZTE directly; if no patch is available within your risk tolerance window, treat the device as EoL and isolate/replace. For DIR-823X replacement, validate that the replacement device is not itself on CISA's Known Exploited Vulnerabilities (KEV) catalog before deployment. A 2-person team can script firmware checksum verification with: 'sha256sum .bin' compared against the vendor advisory hash.

Evidence: Before decommissioning any DIR-823X, if safe to do so via console access, run 'ps' and 'netstat -antp' on the device's embedded Linux shell to document running processes and active connections — tuxnokill Mirai variants typically run as a randomly-named binary in /tmp or /var/run and maintain persistent TCP connections to C2 IPs on

non-standard ports. Capture '/proc/net/tcp' output and '/tmp' directory listing as forensic evidence of the malware binary. For TP-Link devices post-patch, verify the patch closed CVE-2023-1389's LAN-side command injection in the tplinkwifi.net management interface by confirming the patched firmware version matches TP-Link's advisory minimum version.

Recovery — After replacing affected hardware, verify new devices run current, supported firmware from the vendor's official download page. Confirm no lateral movement occurred from compromised routers to internal hosts by reviewing authentication logs and DNS query history for the period of potential exposure. Re-scan the network segment for any residual Mirai-variant indicators before restoring normal traffic flows.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), NIST CA-7 (Continuous Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Run a post-replacement Nmap scan ('nmap -sV -p 23,80,443,8080,7547 ') to confirm management interfaces are not exposed and TR-069 (port 7547) is disabled — Mirai historically exploits TR-069 endpoints. Review Windows Security Event Log on internal hosts for Event ID 4625 (failed logon) and Event ID 4648 (logon using explicit credentials) sourced from the previously compromised router's IP during the exposure window, which would indicate credential brute-forcing lateral movement. Query your DNS resolver's query log (e.g., dnsmasq query log or Windows DNS debug log) for internal hosts that resolved domains matching Mirai C2 patterns (high-entropy domain names, domains registered within 30 days of the incident) originating during the exposure period. Use osquery with 'SELECT * FROM listening_ports WHERE port IN (23, 6667, 6881)' on internal Linux hosts to check for Mirai bot installations that may have spread from the compromised router.

Evidence: Collect DHCP server logs covering the full exposure window (from router deployment or firmware 240126/240820 install date through isolation) to identify all internal hosts that received addresses or communicated through the compromised DIR-823X — these are your lateral movement blast radius candidates. Review internal firewall or switch logs for any TCP/23 (Telnet) scan traffic originating from internal IPs that the compromised router may have pivoted to, which is tuxnokill's primary propagation method. Retain all collected pcap, NetFlow, firewall log, and ARP table data per NIST AU-11 (Audit Record Retention) for a minimum of 90 days to support any post-incident regulatory or insurance requirements.

Post-Incident — Conduct an asset inventory audit to identify any additional end-of-life network devices still in production. Establish a lifecycle management policy requiring vendor support status verification before deployment and a defined replacement schedule for devices approaching EoL. Map this gap to CIS Control 1 (Inventory and Control of Enterprise Assets) and NIST CSF Identify function. Document the 13-month gap between initial CVE disclosure and active exploitation as a data point for patch prioritization SLA review.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-2 (Flaw Remediation), NIST SA-22 (Unsupported System Components), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 1.2 (Address Unauthorized Assets), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Build an EoL tracking spreadsheet cross-referencing your asset inventory against CISA's KEV catalog (downloadable as JSON from cisa.gov/known-exploited-vulnerabilities-catalog) and each vendor's published EoL date list — automate monthly checks with a bash script using 'curl' to fetch the KEV JSON and grep for your device model strings. For CVE-2023-1389 specifically, document the disclosure date (March 2023) versus confirmed active tuxnokill exploitation (March 2026) as a 36-month exploitation lag — use this alongside the DIR-823X 13-month lag to calibrate your network device patch SLA. Submit tuxnokill IOCs (C2 IPs, malware hashes, exploit URIs) to CISA's voluntary sharing portal and, if applicable, to your ISAC for sector-wide benefit, fulfilling NIST IR-6 (Incident Reporting) obligations.

Evidence: Compile the complete incident timeline: first observed tuxnokill honeypot telemetry (Akamai SIRT, March 2026), CVE-2025-29635 disclosure date, CVE-2023-1389 disclosure date (March 2023), DIR-823X EoL date (November 2024), and your organization's device deployment and isolation dates — this timeline is the core artifact for lessons-learned documentation under NIST 800-61r3 §4 and supports insurance claim or regulatory notification if required. Preserve all forensic evidence (pcap files, router console logs, /tmp binary dumps from compromised devices, firewall log exports) with chain-of-custody documentation in case tuxnokill DDoS participation resulted in downstream harm claims.

Detection Guidance

Search firewall and perimeter logs for outbound high-volume UDP traffic originating from router management IPs, characteristic of Mirai DDoS participation. Look for HTTP GET requests from these devices to external IPs fetching binaries (common Mirai staging pattern, MITRE T1105). In SIEM, alert on Telnet login attempts to router IPs from external sources, particularly brute-force sequences. Review DNS logs for queries to unusual domains from router IP space. Akamai SIRT's published campaign analysis includes IOC indicators specific to the tuxnokill infrastructure; cross-reference those against outbound connection logs. For TP-Link CVE-2023-1389 exposure, inspect access logs on affected devices for POST requests to the tddp endpoint with anomalous payloads. Behavioral baseline deviation (routers generating unexpected external connections or elevated CPU/bandwidth) is a secondary signal worth investigating.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.akamai.com/blog/security-research/cve-2025-29635-mirai-campaign-targets-d-link-devices`	Akamai SIRT primary campaign analysis — contains IOCs for tuxnokill infrastructure confirmed via honeypot telemetry	HIGH

Framework Mappings

MITRE-ATTACK

- **T1583.003** — Virtual Private Server
- **T1105** — Ingress Tool Transfer
- **T1498** — Network Denial of Service
- **T1583.005** — Botnet
- **T1498.001** — Direct Network Flood
- **T1059.004** — Unix Shell
- **T1190** — Exploit Public-Facing Application
- **T1059** — Command and Scripting Interpreter

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-10** — Information Input Validation
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

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.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1583.003	Virtual Private Server	Resource-Development
T1105	Ingress Tool Transfer	Command-And-Control
T1498	Network Denial of Service	Impact
T1583.005	Botnet	Resource-Development
T1498.001	Direct Network Flood	Impact
T1059.004	Unix Shell	Execution

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-mirai-campaign-e...	T3
CVE-2025-29635: Mirai Campaign Targets D-Link Devices - Akamai	https://www.akamai.com/blog/security-research/cve-2025-29635-mirai-...	T3
CVE-2023-1389 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2023-1389	T1
Mirai Botnet exploits CVE-2025-29635 to target legacy D-Link routers	https://securityaffairs.com/191135/malware/mirai-botnet-exploits-cv...	T3
Vulnerability Details : CVE-2023-1389	https://www.cvedetails.com/cve/CVE-2023-1389/	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-29635, CVE-2023-1389	T1

Generated 2026-04-23 06:38 UTC by TJS Security Command Center