INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-18 18:47 UTC

Nexcorium Mirai Variant Exploits TBK DVR and EoL TP-Link Router Vulnerabilities in Active IoT Botnet Campaign

THREAT CAMPAIGN | **MEDIUM** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0187
Type	Threat Campaign
CVE ID	CVE-2024-3721, CVE-2017-17215, CVE-2023-33538
Severity	MEDIUM
CVSS Base Score	5.0
EPSS Score	0.8387 (99th percentile)
Affected Products	TBK DVR-4104, TBK DVR-4216, TP-Link TL-WR940N (v2/v4), TP-Link TL-WR740N (v1/v2), TP-Link TL-WR841N (v8/v10), Huawei HG532
Published	2026-04-18T02:01:00
Discovery Source	Rss

Executive Summary

A Mirai-variant botnet called Nexcorium is actively exploiting unpatched and end-of-life TBK DVR and TP-Link router devices to build a DDoS-capable botnet. Organizations with these devices on or near their network perimeters, particularly in surveillance, SMB networking, or remote-access infrastructure, face risk of device compromise, downstream DDoS amplification, and potential lateral movement into adjacent network segments. Direct enterprise risk is moderate but elevated by the 99th-percentile EPSS score on the primary CVE, indicating active, widespread exploitation in the wild.

Technical Analysis

Nexcorium is a Mirai-derived botnet conducting a multi-vector exploitation campaign against IoT hardware. The primary vector exploits CVE-2024-3721 (CWE-77/CWE-78, command injection) in TBK DVR-4104 and DVR-4216 devices; CVSS base scores range from 5.0 to 6.3 depending on scoring version, but the EPSS score of 0.839 (99.3rd percentile) confirms active exploitation at scale. A secondary arm targets end-of-life TP-Link routers, TL-WR940N (v2/v4), TL-WR740N (v1/v2), and TL-WR841N (v8/v10), via CVE-2023-33538, a command injection flaw in these devices' firmware. Huawei HG532 devices are targeted via CVE-2017-17215, a long-exploited remote code execution vulnerability consistent with legacy Mirai playbooks. Exploitation chains combine default or weak credentials (CWE-521) with command injection (CWE-77/CWE-78) to establish

persistent footholds (CWE-912). Compromised devices are enrolled into a botnet awaiting C2 instruction for DDoS operations. All targeted TP-Link models are end-of-life with no vendor patch path available. MITRE ATT&CK techniques observed include T1190 (Exploit Public-Facing Application), T1110.001 (Password Spraying/Brute Force), T1105 (Ingress Tool Transfer), T1498 (Network Denial of Service), T1071.001 (Application Layer Protocol: Web), T1543/T1543.002 (Create/Modify System Process), T1053.003 (Scheduled Task/Job: Cron), T1070.004 (File Deletion), T1098 (Account Manipulation), T1021.004 (Remote Services: SSH), and T1133 (External Remote Services). No patch is available for end-of-life TP-Link models; TBK DVR patch status should be verified against vendor advisories.

Action Checklist

1. Step 1: Containment, Immediately inventory all TBK DVR-4104, DVR-4216, TP-Link TL-WR940N (v2/v4), TL-WR740N (v1/v2), TL-WR841N (v8/v10), and Huawei HG532 devices on your network. Isolate any identified devices from internet-facing exposure and place them behind a restrictive firewall ACL blocking inbound access on management ports (HTTP/HTTPS/Telnet/SSH) until remediated or decommissioned.
2. Step 2: Detection, Query firewall and network flow logs for outbound connections from these devices to anomalous external IPs, particularly on non-standard high ports indicative of C2 communication. Review DHCP logs and asset inventory for unmanaged devices in the affected hardware families. Check for inbound exploitation attempts matching CVE-2024-3721 and CVE-2023-33538 payload patterns in IDS/IPS signatures (Snort/Suricata rules for Mirai-variant command injection). Flag devices exhibiting high outbound UDP/TCP traffic volumes consistent with DDoS participation (T1498).
3. Step 3: Eradication, For TBK DVR-4104 and DVR-4216: apply the vendor firmware update addressing CVE-2024-3721 if available; verify against the TBK vendor advisory. For all end-of-life TP-Link models (TL-WR940N v2/v4, TL-WR740N v1/v2, TL-WR841N v8/v10): no patch is available, decommission and replace with supported hardware. For Huawei HG532: apply firmware patches addressing CVE-2017-17215 if the device is still within vendor support; otherwise retire from service. On all surviving devices, change all default credentials to strong unique passwords before returning to service (CWE-521 remediation).
4. Step 4: Recovery, After patching or replacing devices, validate that no Mirai-variant persistence mechanisms remain: check for unauthorized scheduled tasks (T1053.003), modified init scripts or service definitions (T1543.002), and unexpected binaries downloaded to device storage (T1105). Restore devices from known-good firmware images where possible rather than relying on in-place remediation of potentially compromised hardware. Monitor replaced devices for 72 hours post-restoration for anomalous outbound traffic.
5. Step 5: Post-Incident, This campaign exposes two recurring control gaps: unmanaged IoT/OT devices on network perimeters, and end-of-life hardware without a formal decommission process. Implement a hardware asset lifecycle policy requiring supported firmware for all network-connected devices. Establish a network segmentation baseline that isolates surveillance and SMB-class IoT hardware from corporate segments. Evaluate whether your vulnerability management program includes IoT firmware CVEs, many organizations track server and endpoint CVEs but miss embedded device vulnerabilities until active exploitation occurs.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to senior IR leadership and legal/compliance if network flow analysis confirms any affected TBK DVR or TP-Link device has been actively participating in outbound DDoS flood traffic (T1498) — this creates potential third-party liability and may trigger ISP abuse notifications — or if the compromised device segment has L2/L3 adjacency to systems storing PII, PHI, or PCI-scoped data, which triggers breach notification assessment under applicable regulatory frameworks.
Recovery Notes	After firmware restoration or hardware replacement, validate device integrity by comparing the running firmware version string and SHA256 hash against the vendor's published release manifest before reconnecting to the production network. Monitor all restored or replacement devices via firewall NetFlow for the 72-hour window specifically watching for outbound connections to known Mirai C2 infrastructure — cross-reference destination IPs against the Feodo Tracker botnet C2 blocklist (https://feodotracker.abuse.ch/downloads/ipblocklist.csv — verify URL currency) and the Spamhaus DROP list. If any restored device generates anomalous outbound traffic within the monitoring window, treat it as a re-compromise and escalate to physical hardware replacement rather than attempting further in-place remediation, as Mirai variants can survive firmware flashes on devices with persistent writable storage partitions.
Forensic Artifacts	TBK DVR HTTP access logs: Export from System > Log in the DVR web UI or pull via TFTP; search for POST requests to the authentication/session endpoint with Cookie: uid= values containing shell metacharacters (semicolons, pipes, backticks, $() sequences) — these are the CVE-2024-3721 command injection payload signatures. | TP-Link router system log: Export from Administration > System Log or via syslog forwarding if configured; search for POST requests to /cgi-bin/diagnostic.cgi with pingAddr parameter values containing shell metacharacters — the CVE-2023-33538 exploitation vector — and for any log entries showing unexpected process spawning or wget/tftp download activity following such requests. | Firewall NetFlow or connection-state logs: Filter on source IPs of identified devices for outbound TCP/UDP connections to high ports (4000–65535) with high packet/byte counts to diverse destination /24 subnets — this is the DDoS participation signature (MITRE T1498) and C2 beaconing pattern characteristic of Mirai-variant infections, distinct from normal DVR/router management traffic. | Device filesystem artifacts (if shell accessible): Directory listings of /tmp and writable flash partitions for ELF binaries with random short names, modified /etc/crontabs/root entries containing wget or tftp download commands pointing to external IPs, and modified init.d scripts — these are the Mirai persistence mechanisms (T1053.003, T1543.002, T1105) specific to MIPS/ARM embedded Linux targets like TBK DVRs and TP-Link routers. | DHCP server lease history: Pull full lease history (not just current table) from your DHCP server logs — on Windows DHCP: Event ID 10 (lease assigned) in the Microsoft-Windows-DHCP-Server/Operational log; on ISC DHCP: /var/lib/dhcp/dhcpd.leases — and identify any TBK or TP-Link MAC OUI prefixes that were present on the network during the campaign window (post-March 2024 for CVE-2024-3721) to establish the full scope of potentially exposed devices, including devices that may have been connected and disconnected before your Step 1 inventory.

Per-Action IR Details

Step 1: Containment — Immediately inventory all TBK DVR-4104, DVR-4216, TP-Link TL-WR940N (v2/v4), TL-WR740N (v1/v2), TL-WR841N (v8/v10), and Huawei HG532 devices on your network. Isolate any identified devices from internet-facing exposure and place them behind a restrictive firewall ACL blocking inbound access on management ports (HTTP/HTTPS/Telnet/SSH) until remediated or decommissioned.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), 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 a passive ARP sweep using 'arp-scan -l' or 'nmap -sn 192.168.x.0/24' to enumerate live hosts, then cross-reference MAC OUI prefixes for TBK (no registered OUI — look for unknown vendors), TP-Link (OUI prefix 50:C7:BF, 54:A7:03, EC:08:6B), and Huawei (OUI prefix 48:00:71, 28:6E:D4, 4C:54:99). Immediately apply deny-inbound ACLs on the upstream switch or perimeter firewall for TCP/80, TCP/443, TCP/23, TCP/22, and TCP/8080 originating toward any identified device management IPs. For a 2-person team, prioritize internet-edge devices first — confirm via your ISP/firewall external interface which internal IPs are NAT-forwarded.

Evidence: Before isolating, capture a full packet capture (tcpdump -i -w nexcorium-pre-isolation.pcap -G 300) on the upstream router/firewall interface for each identified device. Document the current WAN-facing IP, any open port scan results (nmap -sV -p 80,443,23,22,8080), and DHCP lease table entries (show ip dhcp binding on Cisco, or /var/lib/dhcp/dhclient.leases on Linux-based firewalls) to establish device presence timeline before containment modifies network state.

Step 2: Detection — Query firewall and network flow logs for outbound connections from these devices to anomalous external IPs, particularly on non-standard high ports indicative of C2 communication. Review DHCP logs and asset inventory for unmanaged devices in the affected hardware families. Check for inbound exploitation attempts matching CVE-2024-3721 and CVE-2023-33538 payload patterns in IDS/IPS signatures (Snort/Suricata rules for Mirai-variant command injection). Flag devices exhibiting high outbound UDP/TCP traffic volumes consistent with DDoS participation (T1498).

NIST Phase: Detection Analysis

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

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

Compensating: Deploy Suricata (free) on a Linux host mirroring the WAN segment with these two rule sets: (1) For CVE-2024-3721 (TBK DVR command injection via cookie header): write a custom rule matching HTTP requests to the TBK management interface containing shell metacharacters in the Cookie: uid= field — e.g., 'alert http any any -> $HOME_NET 80 (msg:"CVE-2024-3721 TBK DVR Command Injection Attempt"; content:"Cookie:"; content:"uid="; pcre:"/uid=[^;]*[;&|`$()]/"; sid:9900001;)'. (2) For CVE-2023-33538 (TP-Link command injection via ping diagnostic POST): match POST requests to /cgi-bin/diagnostic.cgi containing shell metacharacters — e.g., 'alert http any any -> $HOME_NET any (msg:"CVE-2023-33538 TP-Link Diagnostic Command Injection"; http.method; content:"POST"; http.uri; content:"/cgi-bin/diagnostic.cgi"; pcre:"/pingAddr=[^&]*[;&|`$()]/"; sid:9900002;)'. For DDoS participation (T1498), run 'netflow' via ntopng (community edition) or query firewall connection-state tables: on pfSense, run 'pfctl -ss | grep ' and flag any device with >50 concurrent outbound UDP flows to diverse /24 destinations.

Evidence: For CVE-2024-3721 exploitation of TBK DVRs, pull the device's HTTP access log from the DVR web server (typically stored on device flash at /mnt/mtd/log/ or exportable via the web UI under System > Log) and search for POST requests to the authentication endpoint containing anomalous Cookie: uid= values with shell metacharacters. For CVE-2023-33538 on TP-Link routers, extract the router system log (Administration > System Log in the web UI, or via TFTP if management is accessible) and look for POST requests to /cgi-bin/diagnostic.cgi. For Mirai C2 beaconing (T1571), query firewall NetFlow/syslog for outbound TCP connections from device IPs to destination ports in the range 4000–65535 that are not DNS (53), NTP (123), or STUN — Mirai variants commonly beacon to hardcoded C2 IPs on ports such as TCP/48101, TCP/51820, or randomly selected high ports. Capture and hash (sha256sum) any pcap for chain-of-custody.

Step 3: Eradication — For TBK DVR-4104 and DVR-4216: apply the vendor firmware update addressing CVE-2024-3721 if available; verify against the TBK vendor advisory. For all end-of-life TP-Link models (TL-WR940N v2/v4, TL-WR740N v1/v2, TL-WR841N v8/v10): no patch is available — decommission and replace

with supported hardware. For Huawei HG532: apply firmware patches addressing CVE-2017-17215 if the device is still within vendor support; otherwise decommission. On all surviving devices, change all default credentials to strong unique passwords before returning to service (CWE-521 remediation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), NIST IA-5 (Authenticator Management), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

Compensating: For TBK DVR firmware update: download the patched firmware only from the official TBK Security advisory page (do not trust third-party firmware mirrors — Mirai campaigns have historically trojanized firmware images on unofficial sites). Verify the firmware SHA256 hash against the vendor advisory before flashing. For EoL TP-Link devices where replacement hardware is delayed by procurement lead time, implement a compensating control: place the device behind a dedicated VLAN with a deny-all inbound ACL from the internet and a whitelist-only outbound policy (allow DNS to your resolver, NTP to your NTP server, and the specific upstream IPs the device legitimately needs). Document this as a risk-accepted compensating control with a 30-day sunset date. Use 'curl -u admin: http:///cgi-bin/luci/;stok=/rpc' to verify the TP-Link management interface is no longer externally reachable after ACL application. For credential rotation on surviving TBK DVRs, access System > Account Management and set a minimum 16-character random password; document in your password manager.

Evidence: Before flashing or decommissioning, extract and preserve the current firmware version string from each device (TBK DVR: System > Device Information in web UI; TP-Link: Status page showing Firmware Version; Huawei HG532: Device Information tab) and record it in your incident ticket as the confirmed-vulnerable baseline. For any TBK DVR-4104/4216 suspected of active compromise via CVE-2024-3721, attempt to pull the DVR's running process list if the web UI is accessible (some DVR interfaces expose a diagnostics shell): look for unexpected processes named with random 4-8 character strings (typical Mirai binary naming convention, e.g., 'kworker' masquerading, or binaries like 'tftp', 'wget' spawned post-exploitation). Photograph or screenshot the device serial numbers for asset decommission records before physical removal.

Step 4: Recovery — After patching or replacing devices, validate that no Mirai-variant persistence mechanisms remain: check for unauthorized scheduled tasks (T1053.003), modified init scripts or service definitions (T1543.002), and unexpected binaries downloaded to device storage (T1105). Restore devices from known-good firmware images where possible rather than relying on in-place remediation of potentially compromised hardware. Monitor replaced devices for 72 hours post-restoration for anomalous outbound traffic.

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 CP-10 (System Recovery and Reconstitution), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: For TBK DVRs being restored from known-good firmware: perform a full factory reset via the hardware reset button (hold 10+ seconds) before flashing the patched firmware — this clears any Mirai-written files in writable flash partitions. Do NOT restore from a configuration backup taken after the suspected compromise window, as Mirai variants can persist via crontab injection in saved configs. For the 72-hour monitoring window on replacement devices, configure a Suricata or Zeek (free) rule to alert on any outbound connection from the new device IP to non-whitelisted external destinations: 'alert ip any -> ![$DNS_SERVERS,$NTP_SERVERS] any (msg:"New IoT Device Unexpected Outbound"; sid:9900003;)'. Log all alerts to a local file with 'suricata -l /var/log/suricata/ -i ' and review daily. For TP-Link replacements, verify the replacement unit's firmware is current at first boot by checking the TP-Link support page for the specific model and hardware version before connecting to the internet.

Evidence: For TBK DVRs and any router with accessible storage, capture a filesystem listing before restoring firmware: use the device's diagnostic shell or TFTP to pull directory listings of /tmp, /var, and any writable flash mount

points, and hash all binaries found (Mirai typically drops ELF binaries with names mimicking system processes). On TP-Link routers where shell access is possible via the pre-patch CVE-2023-33538 command injection (for forensic purposes only, on an isolated device), run 'ls -la /tmp && cat /etc/crontabs/root && ps' to enumerate Mirai persistence artifacts — document the output verbatim in your incident record. Preserve a copy of the router/DVR's running configuration export (if available) as forensic evidence of the pre-recovery state before factory reset.

Step 5: Post-Incident — This campaign exposes two recurring control gaps: unmanaged IoT/OT devices on network perimeters, and end-of-life hardware without a formal decommission process. Implement a hardware asset lifecycle policy requiring supported firmware for all network-connected devices. Establish a network segmentation baseline that isolates surveillance and SMB-class IoT hardware from corporate segments. Evaluate whether your vulnerability management program includes IoT firmware CVEs — many organizations track server and endpoint CVEs but miss embedded device vulnerabilities until active exploitation occurs.

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 RA-3 (Risk Assessment), NIST CM-8 (System Component Inventory), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), 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: Add IoT/embedded device CVE sources to your vulnerability management intake: subscribe to CISA's Known Exploited Vulnerabilities (KEV) catalog RSS feed (https://www.cisa.gov/known-exploited-vulnerabilities-catalog — note: verify this URL is current) and configure a filter for 'router', 'DVR', 'camera', and 'IoT' keywords. All three CVEs in this campaign (CVE-2024-3721, CVE-2017-17215, CVE-2023-33538) appear or are analogous to KEV-listed vulnerabilities exploited by Mirai variants — your vuln program should have flagged these. For network segmentation of surveillance/IoT hardware with no budget for NAC, use VLAN tagging on managed switches (even consumer-grade managed switches support 802.1Q): create a dedicated IoT VLAN (e.g., VLAN 99) with a firewall rule permitting only outbound traffic to specific upstream IPs needed for device function and blocking all inter-VLAN routing to corporate segments. Document this architecture change in a network diagram update and schedule a quarterly review of IoT VLAN membership against the asset inventory.

Evidence: Conduct a lessons-learned review within 5 business days per NIST 800-61r3 §4, documenting: (1) the date each affected device model was first added to the network vs. the firmware EoL date vs. the date CVEs were published — this gap analysis quantifies the lifecycle policy failure for each device family; (2) whether CVE-2017-17215 (published 2017) for Huawei HG532 was present in your environment for 7+ years unpatched, which constitutes a critical finding for the post-incident report; (3) a count of unmanaged vs. managed devices discovered during Step 1 inventory, which establishes the baseline gap for CIS 1.1 compliance. Retain all incident documentation, pcaps, and firmware hashes for a minimum of 1 year per NIST AU-11 (Audit Record Retention).

Detection Guidance

Focus detection on three signals: (1) Exploitation attempts, monitor IDS/IPS for inbound HTTP POST requests to TBK DVR management interfaces containing shell metacharacters or command injection patterns consistent with CVE-2024-3721; similarly watch for requests targeting CVE-2023-33538 endpoints on TP-Link devices. (2) C2 communication, Mirai variants typically beacon outbound over TCP on ports 23, 2323, 7547, and custom high ports; flag affected device IPs with unusual outbound connection patterns to non-RFC1918 addresses. (3) DDoS participation, alert on sustained high-volume outbound UDP or TCP flood traffic (T1498) originating from IoT device IP ranges. Behavioral indicators include device reboots without user action, configuration changes to scheduled tasks or init services, and new binary downloads to device storage. If your SIEM ingests NetFlow or IPFIX, create a rule alerting on IoT segment egress volume spikes exceeding a 3-sigma baseline. Cross-reference device IPs against current Mirai C2 blocklists maintained by sources such as Spamhaus or abuse.ch Feodo Tracker.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs extracted from available sources`	No specific C2 IPs, domains, or malware hashes were disclosed in the source material available for this item. Monitor Mirai C2 blocklists via abuse.ch Feodo Tracker and Spamhaus for emerging indicators tied to Nexcorium.	LOW

Framework Mappings

MITRE-ATTACK

- **T1021.004** — SSH
- **T1110.001** — Password Guessing
- **T1498** — Network Denial of Service
- **T1071.001** — Web Protocols
- **T1098** — Account Manipulation
- **T1105** — Ingress Tool Transfer
- **T1543** — Create or Modify System Process
- **T1053.003** — Cron
- **T1133** — External Remote Services
- **T1190** — Exploit Public-Facing Application
- **T1070.004** — File Deletion
- **T1543.002** — Systemd Service

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **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
- **CM-7** — Least Functionality

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software
- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1021.004	SSH	Lateral-Movement
T1110.001	Password Guessing	Credential-Access
T1498	Network Denial of Service	Impact
T1071.001	Web Protocols	Command-And-Control
T1098	Account Manipulation	Persistence
T1105	Ingress Tool Transfer	Command-And-Control
T1543	Create or Modify System Process	Persistence
T1053.003	Cron	Execution
T1133	External Remote Services	Persistence
T1190	Exploit Public-Facing Application	Initial-Access
T1070.004	File Deletion	Defense-Evasion
T1543.002	Systemd Service	Persistence

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/mirai-variant-nexcorium-exploits-...	T3
CVE-2024-3721 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-3721	T1
Attackers are exploiting CVE-2024-3721 in TBK DVRs to deploy ...	https://www.facebook.com/thehackernews/posts/attackers-are-exploiti...	T3
CVE-2024-3721 | Tenable®	https://www.tenable.com/cve/CVE-2024-3721	T3
Nexcorium Mirai Variant Weaponizes TBK DVR Vulnerability in ...	https://gbhackers.com/nexcorium-mirai-variant-weaponizes-tbk-dvr-vu...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-3721, CVE-2017-17215, CVE...	T1

Generated 2026-04-18 18:47 UTC by TJS Security Command Center