INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-12 14:16 UTC

C0XMO Botnet Exploiting DD-WRT Router Firmware Vulnerability for DDoS Campaigns

THREAT CAMPAIGN | **HIGH** | CVSS 8.8

SCC Item ID	SCC-CAM-2026-0447
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	8.8
Affected Products	DD-WRT router firmware (unspecified versions); Linux-based IoT devices including routers and DVRs
Published	2026-06-10
Discovery Source	Gemini

Executive Summary

The C0XMO botnet is actively exploiting an authentication bypass vulnerability in DD-WRT router firmware to take over devices without credentials, then enlist them in large-scale DDoS attack infrastructure. Organizations and individuals running DD-WRT on routers, DVRs, and other Linux-based IoT devices are exposed if those devices retain default credentials or face internet-exposed management interfaces. A compromised device becomes a weapon used against third parties, creating operational, reputational, and potential liability risk for the device owner.

Technical Analysis

The C0XMO botnet targets DD-WRT firmware through an unspecified authentication bypass flaw (CWE-287) that allows unauthenticated remote access to device management interfaces. No CVE identifier has been confirmed for this specific vulnerability; no CISA KEV record exists. The authentication bypass vulnerability has not been formally documented in CVE or vendor advisories as of this item's publication date. It is possible this represents a zero-day or a vulnerability under embargo; further confirmation from authoritative sources is recommended. Post-initial-access, the botnet moves laterally using brute-force password spraying against weak or default credentials (CWE-521, T1110.001) across routers, DVRs, and Linux-based IoT devices. Compromised devices are recruited into botnet infrastructure for DDoS campaigns (T1498). Persistence is maintained via system service or init configuration manipulation (CWE-912, T1543). The botnet also exploits internet-facing services for initial access (T1190) and may use default or weak account credentials (T1078.001). Affected versions of DD-WRT are unspecified; no vendor patch or advisory has been confirmed in the available dataset. Source quality is limited: all five sources are Tier 3 (community forums, Reddit, Medium, Stack

Exchange, vendor homepage); no authoritative CVE record, vendor advisory, or threat intelligence report has been identified. The CVSS 8.8 base score is editorial, assigned based on attack scope and impact severity; it is not derived from a vendor or NVD CVSS vector because no official CVE record has been published.

Action Checklist

1. Step 1: Containment. Immediately disable remote management (web UI and SSH) on all internet-facing DD-WRT devices. Block inbound access to ports 80, 443, and 22 on router management interfaces at the network perimeter. Isolate any device suspected of compromise from the production network. Reference: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices).
2. Step 2: Detection. Audit all DD-WRT devices for unexpected outbound traffic spikes (indicative of DDoS participation, T1498), unauthorized account changes, and new or modified startup services (T1543). Review router syslog entries for repeated authentication failures (T1110.001) and unexpected successful logins. Query firewall and NetFlow logs for high-volume outbound UDP/TCP flood patterns from router management IPs. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), D3-LAM (Local Account Monitoring).
3. Step 3: Eradication. Change all default and weak credentials on every DD-WRT device immediately (CIS 5.2, CWE-521 remediation). For devices confirmed compromised, perform a full factory reset and reflash firmware from the official DD-WRT source (https://dd-wrt.com/, verified as of this publication) before reconfiguration. Do not restore from a backup taken after the suspected compromise window. Apply all available DD-WRT firmware updates. Reference: NIST AC-7 (Unsuccessful Logon Attempts), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), D3-CH (Credential Hardening), D3-CRO (Credential Rotation).
4. Step 4: Recovery. After reflashing and recredentialing, re-enable only required services with management interfaces restricted to trusted internal IPs or a dedicated management VLAN. Confirm no unauthorized accounts or startup scripts persist (D3-SICA, System Init Config Analysis). Monitor outbound traffic from recovered devices for 72 hours for anomalous patterns. Verify logging is active and forwarding to a centralized log platform. Reference: NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), NIST AC-17 (Remote Access).
5. Step 5: Post-Incident. Conduct an inventory audit of all DD-WRT and Linux-based IoT devices in the environment (CIS 1.1, Establish and Maintain Detailed Enterprise Asset Inventory). Assess whether any compromised device participated in external DDoS activity; consult legal counsel regarding potential downstream liability and breach notification obligations. Implement a formal process for tracking firmware update availability for all network edge devices (CIS 7.1, Establish and Maintain a Vulnerability Management Process; CIS 7.3, Perform Automated Operating System Patch Management where supported). Consider replacing DD-WRT devices with commercially supported alternatives if a vendor patch for this authentication bypass is not issued within your organization's patching SLA window.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership and legal counsel immediately if NetFlow or firewall logs confirm any DD-WRT device transmitted sustained high-volume outbound UDP/TCP flood traffic to external IPs (indicating active C0XMO DDoS participation), if more than one device shows evidence of authentication bypass exploitation, or if the environment includes devices processing or routing traffic for regulated data (PII, PHI, PCI) that may have been exposed through the compromised management interface.
Recovery Notes	After reflashing each DD-WRT device from a verified clean firmware image, validate the recovered configuration by confirming that remote management interfaces are bound exclusively to the management VLAN or a single trusted internal IP, that NVRAM contains no C0XMO persistence entries in rc_startup or cron variables, and that syslog forwarding is active and producing events on the centralized receiver. Monitor outbound traffic from each recovered device for a minimum of 72 hours using tcpdump or NetFlow on the upstream interface, comparing against the post-recovery baseline — any recurrence of high-PPS outbound UDP/TCP bursts indicates reinfection from a persistence mechanism that survived the reflash (e.g., a JFFS2 partition payload) and requires physical inspection or hardware replacement. If no vendor patch addressing the authentication bypass is published within your organization's defined patching SLA, treat DD-WRT replacement with a commercially supported and actively patched alternative as a risk-driven capital decision, not an optional hardening measure.
Forensic Artifacts	DD-WRT NVRAM dump ('nvram show' output) — C0XMO persistence mechanisms on embedded Linux routers commonly write botnet agent launch commands into the rc_startup or cron NVRAM variables; these survive soft reboots and are the primary persistence artifact specific to this campaign's targeting of DD-WRT firmware. | Contents of /tmp filesystem on the compromised DD-WRT device — DD-WRT's tmpfs (/tmp) is the primary writable runtime location for dropped payloads on this firmware; C0XMO botnet agents targeting embedded Linux commonly stage executables here, making it the first location to image before any reboot or reset action. | Upstream firewall and NetFlow logs showing sustained high-PPS outbound UDP or TCP traffic from the router's WAN IP to rotating external destination IPs — this is the primary network-layer evidence of C0XMO DDoS participation and distinguishes an actively weaponized device from one that was merely compromised but not yet tasked. | DD-WRT syslog HTTP access log entries for the management interface (port 80/443) — the authentication bypass vulnerability produces successful HTTP responses (200 OK) to management interface requests that lack a valid Authorization header or session cookie; these anomalous successful requests without a preceding credential exchange are the exploitation fingerprint in the web server log. | Active TCP/UDP connection table captured via 'cat /proc/net/tcp' and 'cat /proc/net/udp' before isolation — C0XMO botnet agents maintain persistent outbound connections to command-and-control infrastructure; the connection table captures the C2 IP addresses and ports in use at the moment of collection, which are lost upon isolation or reboot.

Per-Action IR Details

Step 1: Containment — Immediately disable remote management (web UI and SSH) on all internet-facing DD-WRT devices. Block inbound access to ports 80, 443, and 22 on router management interfaces at the network perimeter. Isolate any device suspected of compromise from the production network. Reference: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices).

NIST Phase: Containment

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

Controls: CIS 4.4 (IG1/IG2/IG3) — Implement and Manage a Firewall on Servers, CIS 4.5 (IG1/IG2/IG3) — Implement and Manage a Firewall on End-User Devices, NIST AC-17 (Remote Access)

Compensating: For teams without enterprise firewall management: log into each DD-WRT device's web UI (http:///Management.asp) and uncheck 'Remote Management' and 'SSH Management' under Services > Services. At the upstream perimeter, run 'iptables -I FORWARD -d -p tcp --dport 80 -j DROP' (repeat for 443 and 22) on the border Linux firewall or gateway, or apply an inbound ACL on the upstream device blocking those ports to the router management IP. Document each device's management IP and MAC before isolating.

Evidence: Before disabling remote management or isolating any device, capture: (1) active connection table from the DD-WRT device via SSH — run 'cat /proc/net/tcp' and 'netstat -an' to record all established connections including any C2 sessions the C0XMO botnet agent may have open; (2) current running process list via 'ps aux' or 'ps w' (BusyBox syntax) to identify injected botnet daemon processes; (3) contents of /tmp (DD-WRT stores runtime state there — botnet agents commonly drop payloads to /tmp on embedded Linux); (4) active iptables rules via 'iptables -L -n -v' to detect any firewall modifications the botnet made to maintain access or suppress logging. These are entirely volatile and lost upon reboot or isolation.

Step 2: Detection — Audit all DD-WRT devices for unexpected outbound traffic spikes (indicative of DDoS participation, T1498), unauthorized account changes, and new or modified startup services (T1543). Review router syslog entries for repeated authentication failures (T1110.001) and unexpected successful logins. Query firewall and NetFlow logs for high-volume outbound UDP/TCP flood patterns from router management IPs. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), D3-LAM (Local Account Monitoring).

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (IG1/IG2/IG3) — Collect Audit Logs

Compensating: On DD-WRT devices with syslog enabled, forward to a free syslog receiver (syslog-ng or rsyslog on a Linux VM) and grep for authentication events: 'grep -E "dropbear|httpd|login" /var/log/messages'. For outbound flood detection without a SIEM, run Wireshark or tcpdump on the upstream interface: 'tcpdump -i eth0 -nn "src and (udp or tcp)" -w /tmp/capture.pcap' and inspect for high-PPS outbound flows. For NetFlow-free environments, use 'iftop -i ' on the upstream Linux gateway to spot sustained high-bandwidth outbound sessions from the DD-WRT device's WAN IP. Cross-reference DD-WRT's 'Status > Bandwidth' page for anomalous upload spikes.

Evidence: This is a detection/analysis step that does not alter live state, but before any subsequent action: (1) export DD-WRT syslog — look specifically for authentication bypass evidence: HTTP requests to the management interface (port 80/443) that succeeded without a prior credential challenge (indicative of auth bypass exploitation); (2) check /etc/passwd and /etc/shadow on the device for accounts added post-initial-configuration; (3) inspect /jffs/etc/config/ and /nvram for modified startup scripts or nvram variables that the C0XMO botnet uses for persistence (run 'nvram show | grep -E "rc_startup|rc_firewall|cron"'); (4) review upstream firewall NetFlow or connection logs for UDP/TCP flood traffic originating from the router's WAN IP at packet rates exceeding normal browsing baselines — C0XMO DDoS participation produces sustained high-PPS outbound traffic distinguishable from normal NAT'd client traffic.

Step 3: Eradication — Change all default and weak credentials on every DD-WRT device immediately (CIS 5.2, CWE-521 remediation). For devices confirmed compromised, perform a full factory reset and reflash firmware from the official DD-WRT source (https://dd-wrt.com/) before reconfiguration. Do not restore from a backup taken after the suspected compromise window. Apply all available DD-WRT firmware updates. Reference: NIST AC-7 (Unsuccessful Logon Attempts), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), D3-CH (Credential Hardening), D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST AC-7 (Unsuccessful Logon Attempts), CIS 4.7 (IG1/IG2/IG3) — Manage Default Accounts on Enterprise Assets and Software, CIS 5.2 (IG1/IG2/IG3) — Use Unique Passwords

Compensating: For teams without centralized device management: reflash each confirmed-compromised DD-WRT device using the 30-30-30 hard reset procedure (hold reset 30s powered on, 30s powered off, 30s powered on) to clear NVRAM before applying new firmware downloaded directly from dd-wrt.com — verify the downloaded firmware's MD5/SHA256 against the hash published on the DD-WRT release page before flashing. After reflash, use a password manager or a locally-generated random string (e.g., 'openssl rand -base64 16') to set a unique admin password — never reuse the prior credential. Record new credentials in an offline credential store (KeePass or equivalent).

Evidence: Before factory reset or reflash — which destroys all live state — capture the following from each confirmed-compromised device: (1) full NVRAM dump via 'nvram show > /tmp/nvram_dump.txt' and exfiltrate via SCP — this preserves any C0XMO persistence entries written to rc_startup or cron variables; (2) copy all files in /tmp, /jffs, and /opt to external storage — botnet payloads on embedded Linux commonly reside here as they survive soft reboots but not full reflash; (3) capture running process memory where tooling allows (on BusyBox-based DD-WRT this may be limited to 'cat /proc//maps' and 'strings /proc//exe' for identified suspicious PIDs); (4) photograph or screenshot the device's 'Status > Sys-Info' and 'Administration > Logging' pages for administrative record before wiping. Do not restore from any NVRAM backup or config export taken after your identified compromise window.

Step 4: Recovery — After reflashing and recredentialing, re-enable only required services with management interfaces restricted to trusted internal IPs or a dedicated management VLAN. Confirm no unauthorized accounts or startup scripts persist (D3-SICA — System Init Config Analysis). Monitor outbound traffic from recovered devices for 72 hours for anomalous patterns. Verify logging is active and forwarding to a centralized log platform. Reference: NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), NIST AC-17 (Remote Access).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-12 (Audit Record Generation), NIST AC-17 (Remote Access), CIS 8.2 (IG1/IG2/IG3) — Collect Audit Logs, NIST AC-4 (Information Flow Enforcement)

Compensating: Post-reflash validation without enterprise tooling: (1) run 'nvram show | grep -E "rc_startup|rc_firewall|cron"' on the recovered device and confirm output matches only your known-good configuration entries — any unfamiliar commands indicate reinfection or incomplete eradication; (2) on the upstream Linux gateway, run a continuous tcpdump for 72 hours capturing outbound flows from the recovered router's WAN IP: 'tcpdump -i -nn src -w /tmp/recovery_monitor.pcap' with hourly log rotation, reviewing for high-PPS bursts characteristic of C0XMO DDoS participation; (3) confirm DD-WRT syslog is forwarding to your syslog receiver and test by triggering a known-good login and verifying the event appears in the remote log.

Evidence: Recovery steps alter system configuration (re-enabling services, applying access restrictions) but the device has been reflashed — prior volatile state is gone. The evidence focus here is integrity verification of the recovered state: (1) export and retain the post-reflash NVRAM dump as a known-good baseline for future comparison; (2) document the exact firmware version and build date flashed (visible in DD-WRT web UI under 'Status > Router') for asset records; (3) capture the initial 72-hour tcpdump or NetFlow baseline from the recovered device to establish a normal traffic profile — this becomes the comparison point for any future anomaly investigation involving this device.

Step 5: Post-Incident — Conduct an inventory audit of all DD-WRT and Linux-based IoT devices in the environment (CIS 1.1 — Establish and Maintain Detailed Enterprise Asset Inventory). Assess whether any compromised device participated in external DDoS activity; consult legal counsel regarding potential downstream liability. Implement a formal process for tracking firmware update availability for all network edge devices (CIS 7.1 — Establish and Maintain a Vulnerability Management Process, CIS 7.3 — Perform Automated Operating System Patch Management where supported). Consider replacing DD-WRT devices with commercially supported alternatives if a vendor patch for this authentication bypass is not issued within your organization's patching SLA window.

NIST Phase: Post Incident

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

Controls: CIS 1.1 (IG1/IG2/IG3) — Establish and Maintain Detailed Enterprise Asset Inventory, CIS 7.1 (IG1/IG2/IG3) — Establish and Maintain a Vulnerability Management Process, CIS 7.3 (IG1/IG2/IG3) — Perform Automated Operating System Patch Management, NIST AU-11 (Audit Record Retention)

Compensating: For IoT inventory without enterprise asset management tooling: run an nmap scan of your network for devices responding on ports 80, 443, and 22 with DD-WRT-specific HTTP headers ('nmap -sV -p 80,443,22 --script http-title ' and grep results for 'DD-WRT' in page titles or server banners). Supplement with ARP table review ('arp -a') and DHCP lease logs to identify embedded Linux devices by MAC OUI (DD-WRT devices often carry the OUI of the underlying hardware vendor). For firmware update tracking, subscribe to the DD-WRT forum RSS feed and the router hardware vendor's security advisory mailing list — set a calendar reminder for monthly manual checks given the absence of automated patch notification for this firmware.

Evidence: Post-incident evidence focus is on documenting participation in C0XMO DDoS infrastructure for legal and regulatory purposes: (1) retain all upstream firewall and NetFlow logs showing outbound flood traffic from the compromised device's WAN IP, with timestamps, destination IPs, and packet volumes — these establish the scope of any third-party harm; (2) preserve the NVRAM dump and /tmp filesystem snapshots captured during eradication as forensic artifacts demonstrating the nature of the compromise; (3) document the timeline from first anomalous log entry to containment action for the incident report — NIST 800-61r3 §4 requires this for lessons-learned and potential regulatory disclosure assessments; (4) retain syslog records showing authentication events (successful logins without credential challenge) that evidence exploitation of the DD-WRT authentication bypass for at least 12 months per AU-11 requirements.

Detection Guidance

Monitor for these behavioral indicators across your environment. Outbound traffic: look for high-volume UDP or TCP flood traffic originating from router management IPs; this is the primary DDoS participation signal (T1498). Authentication logs: flag repeated failed login attempts followed by a successful login on any DD-WRT device management interface, consistent with password spraying (T1110.001). Service changes: audit /etc/init.d and cron configurations on Linux-based IoT devices for entries not present at baseline (T1543, D3-SICA). Account changes: check for new local accounts or modified admin credentials without a corresponding change record (T1078.001, D3-LAM). Network scanning: detect lateral scanning originating from within the IoT network segment, which may indicate the botnet's propagation phase. Log sources to enable: DD-WRT syslog (forward to SIEM), firewall NetFlow or session logs, and DHCP/ARP tables to detect unexpected new devices. No confirmed IOCs (IPs, domains, hashes) are available in the current dataset; do not implement detection based on fabricated indicators. Version specificity for affected DD-WRT builds is not available from current sources; apply updates to all DD-WRT installations as a precautionary measure. Reference NIST AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting) to ensure these event types are captured.

Framework Mappings

MITRE-ATTACK

- **T1498** — Network Denial of Service
- **T1543** — Create or Modify System Process
- **T1078.001** — Default Accounts
- **T1190** — Exploit Public-Facing Application
- **T1110.001** — Password Guessing

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
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

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

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1498	Network Denial of Service	Impact
T1543	Create or Modify System Process	Persistence
T1078.001	Default Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1110.001	Password Guessing	Credential-Access

Sources

Source	URL	Tier
Question about security patches : r/DDWRT - Reddit	https://www.reddit.com/r/DDWRT/comments/z4yl9p/question_about_secur...	T3
DD-WRT and Router Vulnerabilities | by Imriah - Medium	https://medium.com/ssd-secure-disclosure/dd-wrt-and-router-vulnerab...	T3
View topic - DD-WRT Security Vulnerability Remediation	https://forum.dd-wrt.com/phpBB2/viewtopic.php?t=321995	T3
Is dd-wrt generally more secure than manufacturer's firmware?	https://security.stackexchange.com/questions/49350/is-dd-wrt-genera...	T3
DD-WRT	https://dd-wrt.com/	T3

Generated 2026-06-12 14:16 UTC by TJS Security Command Center