INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-17 08:06 UTC

CVE-2026-12186: A weakness has been identified in GL.iNet GL-MT3000 up to 4.4.5. Affected is the function replace_co...

CVE VULNERABILITY | HIGH | CVSS 8.8

SCC Item ID	SCC-CVE-2026-0320
Type	CVE Vulnerability
CVE ID	CVE-2026-12186
Severity	HIGH
CVSS Base Score	8.8
EPSS Score	0.0202 (78th percentile)
Affected Products	GL.iNet GL-MT3000 firmware versions up to 4.4.5
Published	2026-06-14T21:16:18.483
Discovery Source	Nvd

Executive Summary

A command injection vulnerability in GL.iNet GL-MT3000 routers running firmware versions up to 4.4.5 allows a remote attacker to execute arbitrary operating system commands through the router's Tor Proxy configuration handler. A public exploit is available, raising the likelihood of opportunistic exploitation against unpatched devices. Organizations or remote workers using this router model should treat firmware upgrade to version 4.7 as an immediate priority.

Technical Analysis

CVE-2026-12186 is a command injection vulnerability (CWE-77, CWE-74) in the replace_country function within the /usr/lib/oui-httpd/rpc/tor library on GL.iNet GL-MT3000 firmware through 4.4.5. The vulnerable function processes user-supplied input without sufficient sanitization, enabling injection of arbitrary OS commands via the router's Tor Proxy Service Configuration Handler. The attack is remotely exploitable and does not require authentication in at least some paths, mapping to MITRE ATT&CK T1190 (Exploit Public-Facing Application) and T1059 (Command and Scripting Interpreter). CVSS base score is 8.8 (High). EPSS score is 0.02016 at the 78th percentile, indicating elevated exploitation probability relative to the broader CVE population. A public exploit exists. The vendor responded professionally and released a fix in firmware version 4.7. Sources: NVD (T1), VulnDB (T3).

Action Checklist

1. Step 1: Containment, Identify all GL.iNet GL-MT3000 devices in your environment running firmware 4.4.5 or earlier. Disable or isolate the Tor Proxy Service on affected devices immediately. If remote management interfaces are internet-facing, restrict access via firewall rules to trusted source IPs until firmware is updated. Reference: NIST AC-17 (Remote Access); CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection, Query network logs and DHCP records for GL-MT3000 device presence. Review router administration logs (if accessible via syslog forwarding) for anomalous POST requests to the /usr/lib/oui-httpd/rpc/tor endpoint, particularly those containing shell metacharacters (;, |, $(), backticks) in country parameter fields. Check for unexpected outbound connections from the router's management IP to external hosts. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting); CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication, Upgrade all affected GL.iNet GL-MT3000 devices to firmware version 4.7 via the GL.iNet official administration panel or firmware upgrade mechanism. Verify the upgrade completed successfully and that the device reports version 4.7 post-reboot. If immediate upgrade is not possible, disable the Tor Proxy feature entirely as a compensating control. Reference: NIST SI-2 (Software, Firmware, and Information Integrity); CIS 7.3 (Perform Automated Operating System Patch Management); CIS 7.4 (Perform Automated Application Patch Management).
4. Step 4: Recovery, After firmware upgrade, rotate any credentials or API keys that were accessible from the router's management plane or passed through the device. Re-enable only necessary services and verify Tor Proxy configuration is clean and reflects expected country settings. Monitor outbound traffic from the device for 72 hours post-patch for signs of prior compromise (unexpected DNS queries, persistent outbound sessions). Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting); NIST IA-4 (Account Registration and De-registration).
5. Step 5: Post-Incident, Review the asset inventory to confirm all GL.iNet devices across the environment are tracked and covered by the vulnerability management process. Assess whether remote-management interfaces on network edge devices are unnecessarily exposed to the internet. Update the vulnerability management process to include consumer-grade and prosumer router firmware in patch scope. Reference: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory); CIS 7.1 (Establish and Maintain a Vulnerability Management Process); NIST AC-17 (Remote Access).

Detection Guidance

Query syslog or centralized log management for HTTP POST requests targeting the GL-MT3000 administration interface, specifically to paths associated with the oui-httpd RPC handler and Tor configuration endpoints. Flag any parameter values containing shell metacharacters: semicolons, pipe characters, backticks, dollar signs followed by parentheses, or newline sequences. Look for unexpected process spawning from the router's httpd process in any endpoint detection telemetry if the device feeds into such a system. Monitor for anomalous outbound connections from the router's management IP, particularly to non-standard ports or known Tor exit nodes not consistent with legitimate user configuration. If the device is managed via GL.iNet's cloud management platform, review cloud-side access logs for unexpected API calls. Reference: NIST AU-6; CIS 8.2.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1059** — Command and Scripting Interpreter

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
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures

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

MITRE ATT&CK Mapping

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

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-12186	T1

Source	URL	Tier
CVE-2026-12186 - Exploits & Severity	https://feedly.com/cve/CVE-2026-12186	**T3**

Generated 2026-06-17 08:06 UTC by TJS Security Command Center