INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-22 06:46 UTC

CVE-2026-6560: A security vulnerability has been detected in H3C Magic B0 up to 100R002. This vulnerability affects...

CVE VULNERABILITY | HIGH | CVSS 8.8

SCC Item ID	SCC-CVE-2026-0064
Type	CVE Vulnerability
CVE ID	CVE-2026-6560
Severity	HIGH
CVSS Base Score	8.8
EPSS Score	0.0004 (12th percentile)
Affected Products	H3C Magic B0 up to firmware version 100R002
Published	2026-04-19T07:16:05.973
Discovery Source	Nvd

Executive Summary

A high-severity buffer overflow vulnerability (CVE-2026-6560, CVSS 8.8) has been publicly disclosed in the H3C Magic B0 router running firmware 100R002 or earlier. A public exploit exists, and the vendor has not issued a patch or responded to disclosure. Organizations and consumers using this device on internet-facing networks face remote compromise risk with no vendor-supported remediation path currently available.

Technical Analysis

CVE-2026-6560 is a remotely exploitable stack/heap buffer overflow in the H3C Magic B0 router (firmware up to 100R002). The vulnerability resides in the Edit_BasicSSID function, accessible via the /goform/aspForm endpoint. Improper validation of the 'param' argument allows an attacker to overflow the buffer (CWE-119, CWE-120), potentially enabling remote code execution or device crash. The attack vector is network-accessible, attack complexity is low, and CVSS base score is 8.8 (High). The MITRE ATT&CK technique mapped is T1190 (Exploit Public-Facing Application). A public exploit has been disclosed. The vendor was notified prior to disclosure but did not respond; no patch is available. EPSS score is 0.041% (12.5th percentile), indicating low current exploitation probability in the wild, though the public exploit lowers the bar for opportunistic actors. No CISA KEV listing as of configuration date.

Action Checklist

1. Step 1: Containment, Identify all H3C Magic B0 devices running firmware 100R002 or earlier in your environment. Immediately restrict network access to the /goform/aspForm endpoint; block external access to the router management interface at the perimeter firewall or upstream access control layer. If the device is internet-facing, place it behind a NAT boundary or take it offline if operationally feasible.
2. Step 2: Detection, Query firewall and proxy logs for HTTP POST requests targeting /goform/aspForm with anomalous or oversized 'param' values. Review router syslog output for unexpected reboots, configuration changes, or process crashes that may indicate exploit attempts. If network IDS/IPS is deployed, create a signature for requests to the Edit_BasicSSID endpoint with large payload bodies. As of this writing, no confirmed IOCs have been attributed to active exploitation of this CVE.
3. Step 3: Eradication, No vendor patch is currently available. H3C has not responded to disclosure. Mitigation options are limited to network-level controls: disable remote management access if not required, segment the device to an isolated VLAN, and consider device replacement with a supported model if no fix is issued within an acceptable risk window. Monitor the NVD entry and H3C's official security advisories for patch availability.
4. Step 4: Recovery, After applying network-level mitigations, verify the /goform/aspForm endpoint is no longer reachable from untrusted network segments using an external scan or internal validation. Confirm router configuration integrity by comparing current settings against a known-good baseline. Monitor device logs for at least 30 days post-mitigation for anomalous activity indicative of prior compromise.
5. Step 5: Post-Incident, This vulnerability exposes a control gap in network device lifecycle management: specifically, use of consumer-grade or SOHO routers in environments without compensating controls. Review the device inventory for other H3C Magic series devices. Establish a process for tracking vendor response timelines on disclosed CVEs; where vendors are unresponsive, accelerate replacement timelines. Evaluate whether network segmentation policies adequately isolate management interfaces for all edge devices.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership and legal/compliance if router syslog or firewall logs show any successful POST to /goform/aspForm from an external IP prior to containment, any unexplained router reboot or configuration change during the exposure window, or if the affected H3C Magic B0 device was providing network access to systems handling PII, PHI, PCI-DSS in-scope data, or OT/ICS environments — conditions that may trigger breach notification obligations or regulatory reporting under applicable law.

Recovery Notes	After network-level mitigations are confirmed (endpoint unreachable from untrusted segments via active validation), perform a full configuration integrity comparison against a known-good baseline to rule out attacker-installed persistence such as rogue DNS servers, unauthorized port forwards, or modified wireless credentials — all documented post-exploitation techniques on SOHO routers following buffer overflow compromise. If no clean baseline exists, treat the device configuration as untrusted and perform a factory reset followed by manual reconfiguration from documented settings before returning the device to service. Maintain elevated log monitoring for the H3C device and downstream network segments for 30 days post-mitigation, specifically watching for DNS query anomalies, unexpected outbound connections, or new devices appearing on the network that may indicate a compromised host behind the router was used as a pivot point during any prior exploitation window.
Forensic Artifacts	Upstream firewall or edge router flow logs: Filter for all inbound TCP sessions to the H3C Magic B0 WAN IP on ports 80/443 — the CVE-2026-6560 exploit requires an HTTP POST to /goform/aspForm, so sessions with inbound byte counts significantly above baseline (exploit payload would include an oversized 'param' value designed to overflow the stack buffer in the Edit_BasicSSID handler) are primary forensic evidence of exploitation attempts. | H3C Magic B0 syslog output: Specifically preserve any kernel crash, watchdog reset, or process fault messages — a buffer overflow in the goform CGI handler would likely cause the httpd or goform process to crash, producing a syslog entry before the device reboots; the timestamp of this crash event is the key forensic anchor for establishing exploitation timing. | Full packet capture (pcap) from mirror/SPAN port on upstream switch: A complete pcap of traffic to/from the H3C device's WAN interface during the exposure window preserves the raw exploit payload, enabling post-hoc signature development, attacker infrastructure identification (source IP, TCP handshake timing), and determination of whether the overflow caused a crash-only condition or resulted in code execution (indicated by subsequent outbound C2 traffic from the router's IP). | H3C device running configuration export (pre- and post-mitigation): Compare 'display current-configuration' output against the factory default or a prior known-good backup — attacker modification of DNS server settings (to rogue resolvers for traffic interception) or addition of unauthorized port forwarding rules are the most common persistence mechanisms following SOHO router buffer overflow exploitation and would appear as configuration deltas. | DHCP lease table and ARP cache from the H3C device: Export 'display dhcp server ip-in-use' and 'display arp' output immediately during containment — if the router was compromised, the attacker may have introduced a rogue device onto the LAN segment behind it, and an unexpected MAC address or IP lease in the table during the exposure window is forensic evidence of lateral movement or attacker-controlled device placement behind the exploited router.

Per-Action IR Details

Step 1: Containment — Identify all H3C Magic B0 devices running firmware 100R002 or earlier in your environment. Immediately restrict network access to the /goform/aspForm endpoint; block external access to the router management interface at the perimeter firewall or upstream access control layer. If the device is internet-facing, place it behind a NAT boundary or take it offline if operationally feasible.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment, Eradication, and Recovery: Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), 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 80,443,8080,8443 --open -oG -' to identify H3C Magic B0 devices responding on common management ports, then cross-reference against DHCP lease files or ARP tables ('arp -a' on the upstream

gateway). At the perimeter firewall, create an explicit DENY ACL for TCP ports 80/443 destined to the H3C device's WAN IP, and add a rule blocking POST requests to '/goform/aspForm' if your firewall supports L7 string matching (e.g., iptables with '--string' match module: 'iptables -I FORWARD -p tcp --dport 80 -m string --string "/goform/aspForm" --algo bm -j DROP'). Verify isolation with 'curl -m 5 http:///goform/aspForm' from an external vantage point — a timeout or connection refused confirms the block.

Evidence: Before isolating the device, capture the current router management interface HTTP response headers and any exposed firmware version strings via 'curl -I http:///' and save output. Export the full routing table and ARP cache from the H3C device CLI if accessible ('display arp', 'display ip routing-table'). Capture a full packet capture of traffic to/from the device's WAN interface for the prior 24-48 hours from the upstream switch or firewall (pcap via tcpdump or Wireshark on mirror/SPAN port) — the buffer overflow exploit for CVE-2026-6560 targets the 'param' parameter in POST requests to /goform/aspForm and would appear as anomalously large HTTP POST bodies in this capture. Preserve firewall connection state logs showing all inbound sessions to the device's management port before ACLs are applied.

Step 2: Detection — Query firewall and proxy logs for HTTP POST requests targeting /goform/aspForm with anomalous or oversized 'param' values. Review router syslog output for unexpected reboots, configuration changes, or process crashes that may indicate exploit attempts. If network IDS/IPS is deployed, create a signature for requests to the Edit_BasicSSID endpoint with large payload bodies. Note: No confirmed IOCs (IPs, hashes, domains) have been publicly attributed to active exploitation of this CVE as of this writing.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Detecting Incidents and Analyzing Incident Signs

Controls: NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: If no SIEM is available, use the following pipeline on the syslog server or firewall log host: 'grep -i "aspForm" /var/log/firewall.log | awk '{print $0}' | grep -i "POST"' to isolate relevant requests. For oversized param detection, use: 'awk 'length($0) > 500' /var/log/http_access.log | grep aspForm' as a rough heuristic for abnormally large POST bodies targeting this endpoint. Deploy Suricata (free) with a custom rule targeting this specific endpoint and payload pattern: 'alert http any any -> $HOME_NET any (msg:"CVE-2026-6560 H3C Magic B0 aspForm Exploit Attempt"; flow:to_server,established; http.method; content:"POST"; http.uri; content:"/goform/aspForm"; http.request_body; isdataat:256,relative; sid:9026560; rev:1;)'. Forward H3C syslog to a central rsyslog server and monitor for keywords 'reboot', 'crash', 'segfault', or 'panic' using: 'tail -f /var/log/h3c_syslog.log | grep -Ei "reboot|crash|segfault|config changed"'.

Evidence: Collect H3C Magic B0 syslog output covering the full exposure window — specifically look for syslog facility kern or daemon messages indicating process crashes or watchdog-triggered reboots, which are consistent with a failed or partially successful buffer overflow exploit against the goform CGI handler. Extract firewall flow logs showing source IPs, byte counts, and connection durations for all inbound sessions to TCP/80 or TCP/443 on the H3C device — exploit attempts for this CVE would show POST requests with Content-Length or actual body sizes significantly exceeding normal management traffic (typically under 1KB). If the router was reachable via Telnet or SSH, capture authentication logs for any successful sessions from unexpected source IPs. Preserve a full copy of the router's running configuration ('display current-configuration' if CLI is accessible) as a baseline for detecting post-exploit configuration tampering such as rogue SSID injection or DNS hijacking — both are consistent with post-exploitation of a SOHO router buffer overflow.

Step 3: Eradication — No vendor patch is currently available. H3C has not responded to disclosure. Mitigation options are limited to network-level controls: disable remote management access if not required, segment the device to an isolated VLAN, and consider device replacement with a supported model if no fix is issued within an acceptable risk window. Monitor the NVD entry and H3C's official security advisories for patch availability.

NIST Phase: Eradication

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

Controls: NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Because no H3C firmware patch exists for CVE-2026-6560, eradication must be achieved through network-layer enforcement rather than software remediation. On the H3C device CLI, disable the web management interface entirely if the device supports it ('undo ip http enable' or equivalent H3C VRP command) to prevent the /goform/aspForm CGI from accepting any connections. Create a dedicated management VLAN (e.g., VLAN 999) using the upstream managed switch and assign only the H3C device and an authorized management workstation to that VLAN, blocking all inter-VLAN routing from production networks using ACLs on the Layer 3 switch. Set a recurring calendar reminder (30-day interval) to check https://www.nvd.nist.gov/vuln/detail/CVE-2026-6560 and H3C's security portal for patch status; if no patch is issued within your organization's defined risk acceptance window (recommend 60-90 days for a CVSS 8.8 unpatched device), initiate procurement for a replacement device from a vendor with an active security response program.

Evidence: Before executing VLAN segmentation or disabling the management interface, take a final full configuration export from the H3C device to establish a tamper-evidence baseline — hash the output file with 'sha256sum config_export.txt' and store it in your incident case file. Verify no unauthorized static routes, rogue DNS entries, or unknown SSID configurations have been added to the device, which would indicate the buffer overflow was successfully exploited prior to containment and the attacker modified router settings (a common post-exploitation persistence mechanism on SOHO routers). If the device was fully internet-exposed before containment, treat it as potentially compromised and capture volatile memory state if the device supports any diagnostic dump function before making configuration changes.

Step 4: Recovery — After applying network-level mitigations, verify the /goform/aspForm endpoint is no longer reachable from untrusted network segments using an external scan or internal validation. Confirm router configuration integrity by comparing current settings against a known-good baseline. Monitor device logs for at least 30 days post-mitigation for anomalous activity indicative of prior compromise.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Eradication and Recovery: Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CA-7 (Continuous Monitoring), NIST AU-11 (Audit Record Retention), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 8.2 (Collect Audit Logs)

Compensating: Validate that /goform/aspForm is blocked from untrusted segments using: 'curl -X POST -d "param=$(python3 -c 'print("A"*300)')" http:///goform/aspForm --connect-timeout 5 -v' from an external or untrusted-segment host — a connection timeout or TCP RST (not a 200 OK or 500 error) confirms the network-layer block is effective. Compare current router configuration against your saved baseline using 'diff --script http-title' daily and alert on any change in the management interface's HTTP response, which could indicate a firmware modification or attacker-installed backdoor.

Evidence: Retain all syslog output, firewall flow logs, and packet captures collected during containment and detection phases for a minimum of 90 days per NIST AU-11 (Audit Record Retention) to support any subsequent forensic investigation or regulatory inquiry. Specifically preserve the timestamp-correlated sequence of any router reboots identified during detection — a reboot followed immediately by configuration changes to DNS or wireless settings within the exposure window is strong forensic evidence of successful CVE-2026-6560 exploitation and subsequent attacker persistence. Document the exact date and time network mitigations were applied as the 'containment timestamp' in your incident record to establish the exposure window boundary for any downstream breach notification analysis.

Step 5: Post-Incident — This vulnerability exposes a control gap in network device lifecycle management: specifically, use of consumer-grade or SOHO routers in environments without compensating controls. Review the device inventory for other H3C Magic series devices. Establish a process for tracking vendor response timelines on disclosed CVEs; where vendors are unresponsive, accelerate replacement timelines. Evaluate whether network segmentation policies adequately isolate management interfaces for all edge devices.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons Learned and Evidence Retention

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-2 (Flaw Remediation), 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: Expand the asset inventory query beyond H3C Magic B0 to cover all H3C Magic series devices (B1, R1, NX series) using 'nmap -sV --script banner ' and matching HTTP server banners or SNMP sysDescr strings containing 'H3C' or 'Magic' — CVE-2026-6560's root cause (unsafe input handling in the goform CGI framework) is architecturally common across H3C SOHO product lines and may affect related models. Formalize a vendor SLA tracking spreadsheet with columns for CVE ID, affected product, disclosure date, vendor acknowledgment date, patch release date, and escalation action — for unresponsive vendors like H3C in this case, set a 30-day review trigger to reassess risk and accelerate replacement procurement. Reference CIS 2.2 (Ensure Authorized Software is Currently Supported) as the policy basis for removing unsupported devices from the authorized inventory.

Evidence: Compile the complete incident timeline from initial exposure through containment for the lessons-learned record, including: the date CVE-2026-6560 was publicly disclosed, the date your organization identified affected H3C Magic B0 devices in inventory, the elapsed time to containment, and any evidence of exploit attempts detected in logs — this gap analysis directly informs updates to detection SLAs and asset visibility procedures under NIST IR-8 (Incident Response Plan). Retain all forensic artifacts, configuration exports, and log archives collected during this incident as supporting evidence for the post-incident review, and cross-reference them against your written IR plan to identify procedural gaps (e.g., absence of a network device firmware tracking process or missing syslog forwarding from edge routers, both of which this incident likely exposed).

Detection Guidance

As of this writing, no confirmed IOCs have been attributed to active exploitation of CVE-2026-6560. Detection should focus on behavioral indicators: monitor HTTP server logs on the router (if accessible) for POST requests to /goform/aspForm with unusually large 'param' field values. At the network perimeter, alert on unexpected outbound connections from H3C Magic B0 device IP addresses, which may indicate post-exploitation callback activity. Check for unexpected device reboots or configuration changes in router management logs. If a SIEM is ingesting edge device logs, create a detection rule for repeated failed requests or large-body POST requests to the affected endpoint. Given the low EPSS score (0.041%), active exploitation is not currently observed at scale, but the presence of a public exploit makes opportunistic scanning plausible.

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-2026-6560	T1
CVE Record: CVE-2026-6560	https://www.cve.org/CVERecord?id=CVE-2026-6560	T3
CVE Alert: CVE-2026-6560 - H3C - Magic B0	https://www.redpacketsecurity.com/cve-alert-cve-2026-6560-h3c-magic...	T3
CVE-2026-6560 - High Vulnerability	https://www.thehackerwire.com/vulnerability/CVE-2026-6560/	T3
CVE-2026-6560 - H3C Magic B0 - Buffer Overflow	https://leakycreds.com/vulnerability/CVE-2026-6560	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-22 06:46 UTC by TJS Security Command Center