INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-22 06:47 UTC

CVE-2026-6563: A vulnerability has been found in H3C Magic B1 up to 100R004. The affected element is the function S...

CVE VULNERABILITY | HIGH | CVSS 8.8

SCC Item ID	SCC-CVE-2026-0065
Type	CVE Vulnerability
CVE ID	CVE-2026-6563
Severity	HIGH
CVSS Base Score	8.8
EPSS Score	0.0004 (12th percentile)
Affected Products	H3C Magic B1 up to firmware version 100R004
Published	2026-04-19T09:16:11.000
Discovery Source	Nvd

Executive Summary

A buffer overflow vulnerability in H3C Magic B1 routers (firmware 100R004 and earlier) allows remote attackers to execute arbitrary code without authentication. The exploit has been publicly disclosed, and H3C has not issued a patch or acknowledged the report. Organizations with these devices internet-facing or on branch/home office networks face immediate risk of device compromise, network pivoting, and traffic interception.

Technical Analysis

CVE-2026-6563 is a stack/heap buffer overflow (CWE-119, CWE-120) in the H3C Magic B1 router's SetAPWifiorLedInfoById function, reachable via HTTP POST to /goform/aspForm. Sending an oversized or malformed value in the param argument causes a buffer overflow condition. CVSS base score: 8.8 (High). No authentication is required for exploitation based on the scoring vector. The vulnerability maps to MITRE ATT&CK T1190 (Exploit Public-Facing Application) and T1203 (Exploitation for Client Execution). Affected versions: H3C Magic B1 up to firmware 100R004. EPSS score: 0.00041 (12.5th percentile), in-the-wild exploitation not yet widely observed, but public exploit availability accelerates that timeline. No patch is available. H3C did not respond to pre-disclosure notification. No CISA KEV listing as of the configuration date.

Action Checklist

1. Containment: (1) Identify all H3C Magic B1 devices running firmware 100R004 or earlier in your environment. (2) Immediately restrict inbound access to the /goform/aspForm endpoint at the network perimeter. (3) If devices are internet-facing, place them behind a NAT boundary or firewall rule blocking external HTTP/HTTPS access to the management interface.
2. Detection: (1) Query firewall and web proxy logs for POST requests targeting /goform/aspForm on H3C Magic B1 IP addresses. (2) Look for oversized or malformed 'param' field values. (3) Check DHCP/ARP tables and network flow data for unexpected outbound connections originating from these devices, which may indicate post-exploitation activity.
3. Eradication: (1) No vendor patch is available. (2) Remove or replace H3C Magic B1 devices in high-risk network positions (internet-facing, adjacent to sensitive segments) until H3C issues a fix. (3) If replacement is not immediately possible, disable remote management interfaces and enforce strict ingress filtering on all device-accessible ports.
4. Recovery: (1) After isolation or replacement, verify no lateral movement occurred from affected devices. (2) Review authentication logs on adjacent systems for anomalous access patterns timed with any suspicious traffic to the router. (3) Restore normal network operations only after confirming device integrity or completing hardware replacement.
5. Post-Incident: (1) Document this event as a case study in unpatched SOHO/branch router risk. (2) Review your device inventory process for visibility gaps on embedded network hardware. (3) Assess whether your vulnerability management program includes firmware versioning for network edge devices, and whether vendor responsiveness is evaluated during procurement.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/compliance team immediately if NetFlow or firewall logs confirm any outbound connections from H3C Magic B1 devices to external IPs following a POST to /goform/aspForm, as this indicates successful exploitation and potential network-wide compromise requiring breach notification assessment under applicable regulations (GDPR, state breach laws, HIPAA if PHI traverses the affected segment).
Recovery Notes	After replacing or isolating all H3C Magic B1 devices running firmware 100R004 or earlier, monitor all previously adjacent LAN hosts for 14 days for anomalous authentication attempts, new scheduled tasks, or unexpected outbound connections that may indicate a threat actor established persistence on LAN hosts before the router was isolated. Verify DNS resolution integrity on the segment by comparing current DNS server assignments on LAN hosts against your known-good baseline, as a compromised H3C router could have served rogue DHCP/DNS responses to redirect traffic. Confirm hardware replacement completion in your asset inventory and close the CVE-2026-6563 finding only upon verified removal of all 100R004 firmware devices from network-connected positions.

Forensic Artifacts	Firewall and web proxy logs containing POST requests to /goform/aspForm with oversized or malformed 'param' field payloads — the specific URI path and parameter name are the primary indicators of CVE-2026-6563 exploitation attempts against the H3C Magic B1 goform handler | NetFlow or sFlow records for the H3C Magic B1's WAN interface showing any NEW outbound TCP sessions to external IPs in the minutes following a suspicious POST to /goform/aspForm — these connections represent post-exploitation reverse shell or C2 traffic established via the buffer overflow | ARP cache and DHCP binding table snapshots from the LAN segment, preserved before device isolation, to detect any unauthorized MAC addresses introduced by an attacker pivoting through the compromised H3C router onto the internal network | Router syslog output (if the H3C Magic B1 was configured to forward syslog externally) covering the exploitation window, specifically process crash/restart events or authentication events that would correlate with successful buffer overflow code execution triggering a service restart on the device | Flash memory forensic image of the H3C Magic B1 (acquired via UART console or JTAG if feasible before replacement), analyzed with binwalk to detect injected binaries, modified startup scripts, or implanted backdoor configurations installed by an attacker after achieving arbitrary code execution via CVE-2026-6563

Per-Action IR Details

Containment — Identify all H3C Magic B1 devices running firmware 100R004 or earlier in your environment. Immediately restrict inbound access to the /goform/aspForm endpoint at the network perimeter. If devices are internet-facing, place them behind a NAT boundary or firewall rule blocking external HTTP/HTTPS access to the management interface.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run a network sweep using nmap to enumerate HTTP/HTTPS management interfaces on RFC1918 ranges: 'nmap -p 80,443,8080 --open -sV --script http-title 192.168.0.0/16 | grep -i H3C'. Cross-reference DHCP lease tables (router or server logs) for MAC OUI prefix matching H3C devices (OUI: 00-0F-E2, 58-69-6C). Apply a blocking ACL on your upstream firewall or edge switch: deny TCP any [H3C-IP] eq 80 443. On a Linux-based perimeter device use iptables: 'iptables -I FORWARD -d [H3C-IP] -p tcp --dport 80 -j DROP'. Verify the block with 'curl -m 5 http://[H3C-IP]/goform/aspForm' returning connection refused.

Evidence: Before isolating the device, capture the current ARP cache ('arp -a' or 'ip neigh show') and DHCP binding tables to establish a device inventory baseline. Export firewall connection state tables to preserve any active sessions to/from the H3C Magic B1 management IP. If the device is accessible, capture the running config and firmware version string via the management interface or SNMP ('snmpwalk -v2c -c public [H3C-IP] sysDescr') before network isolation severs access. Document the device's WAN IP, LAN IP, and MAC address as pivot reference points for subsequent lateral movement analysis.

Detection — Query firewall and web proxy logs for POST requests targeting /goform/aspForm on H3C Magic B1 IP addresses. Look for oversized or malformed 'param' field values. Check DHCP/ARP tables and network flow data for unexpected outbound connections originating from these devices, which may indicate post-exploitation activity.

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-2 (Event Logging), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Query firewall syslog for POST requests to /goform/aspForm using grep: 'grep -E "POST.*goform/aspForm" /var/log/firewall.log | awk "{print $1, $2, $NF}"'. Filter for requests with a Content-Length or

body size exceeding 512 bytes, which would indicate a buffer overflow attempt against the vulnerable param field. For NetFlow/IPFIX without a SIEM, use ntopng (free community edition) or 'tcpdump -i eth0 -w h3c_capture.pcap host [H3C-IP]' followed by Wireshark display filter 'http.request.method == POST && http.request.uri contains "/goform/aspForm"'. For post-exploitation outbound anomaly detection, use 'netflow' data or router syslog to flag any NEW outbound TCP sessions from the H3C device IP to non-DNS, non-NTP external destinations, which would indicate a reverse shell or C2 beacon established after successful buffer overflow exploitation.

Evidence: Preserve raw firewall and proxy logs covering at minimum 30 days prior to detection, specifically filtering POST requests to /goform/aspForm with anomalously large param field payloads that would trigger the buffer overflow in the H3C Magic B1 goform handler. Capture full NetFlow or sFlow records for the H3C device's WAN and LAN interfaces to identify any outbound connections to external IPs that postdate the earliest suspicious POST request — these connections represent post-exploitation C2 or data exfiltration from a compromised router. Export ARP table history to identify any new MAC-to-IP mappings appearing on the LAN segment after the suspected compromise window, which could indicate an attacker-controlled device inserted via the compromised router.

Eradication — No vendor patch is available. Remove or replace H3C Magic B1 devices in high-risk network positions (internet-facing, adjacent to sensitive segments) until H3C issues a fix. If replacement is not immediately possible, disable remote management interfaces and enforce strict ingress filtering on all device-accessible ports.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality) — referenced from CM family per 800-53r5, CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Since no H3C patch exists for CVE-2026-6563, treat device replacement as the primary eradication action. If hardware replacement is delayed, access the H3C Magic B1 management UI and disable the web-based management interface if a toggle is available; then apply upstream ACLs blocking all inbound TCP 80/443/8080/8443 to the device's LAN management IP from any source. Use a Sigma rule to trigger on any resumed POST traffic to /goform/aspForm as a regression indicator: write a Sigma rule matching http_method=POST and cs-uri-stem containing '/goform/aspForm' targeting the device IP. Document the compensating control formally with a risk acceptance sign-off since the underlying CVE-2026-6563 vulnerability remains unpatched in firmware.

Evidence: Before physically removing or factory-resetting the H3C Magic B1, acquire a forensic image of the device's flash memory if tooling permits (UART/JTAG console access or firmware extraction via binwalk on a dumped image) to preserve evidence of any implanted backdoor, modified cron job, or injected process that an attacker may have installed post-exploitation via the buffer overflow. Document the firmware version string confirming 100R004 or earlier. If the device exhibited outbound anomalies identified in the detection step, treat it as compromised and do not reconnect it to any network segment prior to imaging.

Recovery — After isolation or replacement, verify no lateral movement occurred from affected devices. Review authentication logs on adjacent systems for anomalous access patterns timed with any suspicious traffic to the router. Restore normal network operations only after confirming device integrity or completing hardware replacement.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), CIS 6.2 (Establish an Access Revoking Process), CIS 5.3 (Disable Dormant Accounts)

Compensating: On Windows systems adjacent to the H3C Magic B1's LAN segment, query the Security Event Log for lateral movement indicators time-correlated to the suspicious /goform/aspForm POST window: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4624,4625,4648,4776) -and $_.TimeCreated -gt [datetime]"[T0-suspicious]"} | Select-Object TimeCreated, Id, Message | Export-Csv lateral_auth.csv'. On Linux hosts, run 'last -F' and 'grep -E "Accepted|Failed" /var/log/auth.log' filtered to the same window. For network devices, pull ARP cache history and compare MAC addresses seen on the LAN segment post-compromise to your CIS 1.1 asset

inventory baseline to identify any unauthorized devices that may have been introduced by a threat actor pivoting through the compromised H3C router.

Evidence: Before restoring the network segment to full operational status, collect Windows Security Event Log entries (Event IDs 4624, 4625, 4648, 4776, 4768, 4769) and Linux auth.log entries from all hosts on the same LAN segment as the H3C Magic B1 for the 72-hour window surrounding the earliest detected suspicious POST to /goform/aspForm. Also collect DNS query logs from the segment's resolver to identify any unusual domain resolutions originating from the H3C device IP, which would indicate DNS-based C2 established post-exploitation. These logs must be preserved to an isolated log store before the device is replaced, as replacement terminates the router's own connection state and syslog history.

Post-Incident — Document this event as a case study in unpatched SOHO/branch router risk. Review your device inventory process for visibility gaps on embedded network hardware. Assess whether your vulnerability management program includes firmware versioning for network edge devices, and whether vendor responsiveness is evaluated during procurement.

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-5 (Security Alerts, Advisories, and Directives), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Extend your asset inventory (CIS 1.1) to include firmware version fields for all network edge devices by running a scheduled nmap scan: 'nmap -sV -p 80,443 --script http-title,banner [network-range] -oX edge_devices.xml' and parsing output for embedded device banners. Import results into a spreadsheet tracking vendor, model, firmware version, and CVE exposure. For procurement process improvement, add a mandatory field to your vendor evaluation checklist: 'Vendor patch SLA and disclosure policy for CVEs affecting this product' — CVE-2026-6563 demonstrates that H3C did not acknowledge or patch this vulnerability, which constitutes a procurement risk factor for future H3C device purchases. Schedule a quarterly firmware review against CISA KEV and NVD for all edge devices using a free script querying the NVD API: 'curl https://services.nvd.nist.gov/rest/json/cves/2.0?keywordSearch=H3C+Magic'.

Evidence: Compile the complete incident timeline from initial CVE-2026-6563 disclosure to containment completion, including: the date range of exposure (devices running firmware 100R004 or earlier), the earliest suspicious POST request to /goform/aspForm identified in firewall logs, any confirmed or suspected post-exploitation outbound connections, and the containment/replacement completion date. This timeline, combined with the asset inventory gaps identified during containment (Step 1), constitutes the lessons-learned artifact required by NIST IR-4 and forms the basis for updating your vulnerability management program to include embedded firmware versioning for SOHO and branch-office network hardware.

Detection Guidance

Query firewall and proxy logs for HTTP POST requests to /goform/aspForm on any H3C Magic B1 device IP. Flag requests where the 'param' field length exceeds normal bounds or contains binary/shellcode-like content. Monitor outbound traffic from router management IPs for unexpected DNS queries, reverse shell patterns (outbound connections on non-standard ports), or traffic to external IPs outside your known infrastructure. On IDS/IPS, write a signature targeting POST /goform/aspForm with oversized param values. MITRE T1190 detection context: correlate web server access logs on the router (if accessible via syslog export) with any subsequent anomalous internal network behavior.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1203** — Exploitation for Client Execution

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-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation

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

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
T1190	Exploit Public-Facing Application	Initial-Access
T1203	Exploitation for Client Execution	Execution

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-6563	T1
CVE-2026-6563 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-6563	T3
CVE-2026-6563 - Exploits & Severity - Feedly	https://feedly.com/cve/CVE-2026-6563	T3
CVE-2026-6563 - High Vulnerability - TheHackerWire	https://www.thehackerwire.com/vulnerability/CVE-2026-6563/	T3
CVE-2026-6563 Security Vulnerability Analysis & Exploit Details	https://cve.akaoma.com/cve-2026-6563	T3

Generated 2026-04-22 06:47 UTC by TJS Security Command Center