INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-27 06:09 UTC

CVE-2026-12485: Stack Overflow in GeoVision GV-I/O Box 4E DVRSearch Service Enables Unauthenticated Remote Code Execution

CVE VULNERABILITY | **CRITICAL** | CVSS 10.0

SCC Item ID	SCC-CVE-2026-0357
Type	CVE Vulnerability
CVE ID	CVE-2026-12485
Severity	CRITICAL
CVSS Base Score	10.0
EPSS Score	0.0044 (35th percentile)
Affected Products	GeoVision GV-I/O Box 4E (smart embedded device); specific firmware versions not specified in available data
Published	2026-06-24T05:17:25.973
Discovery Source	Nvd

Executive Summary

A critical stack-based buffer overflow in the GeoVision GV-I/O Box 4E DVRSearch service allows any unauthenticated attacker on the network to execute arbitrary code on the device by sending a single crafted UDP packet. The vulnerability carries a maximum CVSS score of 10.0 and requires no credentials, no user interaction, and no special access; any host that can reach UDP port 10001 is a potential attacker. Organizations with these devices on operational technology networks, building management systems, or perimeter-accessible segments face immediate risk of device compromise, physical access system manipulation, and lateral movement.

Technical Analysis

CVE-2026-12485 (CWE-121: Stack-Based Buffer Overflow) affects the DVRSearch service in the GeoVision GV-I/O Box 4E, a smart embedded device with 4 inputs and 4 relay outputs controllable via Ethernet and RS-485. The service runs by default and listens on UDP port 10001. The service accepts up to 1460 bytes into a local buffer and stores the data in a global variable (g_network_config->ip_addr). The vulnerability is triggered in the IP field handling routine: strlen(g_network_config->ip_addr) determines copy length, which is then passed to an unchecked memcpy into a 36-byte stack buffer (reply_buf[36]), allowing complete stack overwrite with

attacker-controlled data. No authentication is required. CVSS base score is 10.0; EPSS score is 0.00436 (34.9th percentile) at time of publication. GeoVision has not published an independent CVSS assessment; NVD base score of 10.0 is the authoritative rating at time of publication. Three related CVEs, CVE-2026-12846, CVE-2026-12847, and CVE-2026-12848, are consolidated alongside this issue, indicating a broader vulnerability surface in the same device or service. Specific vulnerable firmware versions are not defined in available source data. No vendor CVSS vector or patch advisory has been identified in the provided data. Sources: NVD (T1) for all four CVE IDs.

Action Checklist

1. Step 1: Containment. Immediately identify all GeoVision GV-I/O Box 4E devices on your network using asset inventory records (CIS 1.1). Block inbound and outbound UDP port 10001 at the network perimeter and on internal segmentation boundaries using host-based and server firewalls (CIS 4.4, CIS 4.5, NIST AC-4). Isolate any device that cannot be immediately firewalled to a restricted VLAN with no internet exposure.
2. Step 2: Detection. Query network flow logs and firewall logs for UDP traffic to port 10001 targeting known GV-I/O Box 4E device IPs. Alert on any external source IP communicating with these devices. Review syslog output from affected devices for unexpected process crashes, reboots, or anomalous relay output activity. Monitor for lateral movement originating from device IP addresses (NIST AU-6, AU-2).
3. Step 3: Eradication. Check the GeoVision vendor portal or contact GeoVision support directly for firmware updates addressing CVE-2026-12485, CVE-2026-12846, CVE-2026-12847, and CVE-2026-12848. If a firmware update is not yet available, disable the DVRSearch service on UDP port 10001 where the device configuration permits, or enforce network-level block as a compensating control (NIST SI-4, CIS 7.1, CIS 7.2).
4. Step 4: Recovery. After applying firmware updates or compensating controls, verify UDP port 10001 is no longer reachable from unauthorized segments using a port scanner run from an external and internal vantage point. Confirm device relay outputs and input states are operating as expected and have not been manipulated. Re-enable monitored network access only after verification. Retain logs from the isolation period for post-incident review (NIST AU-11, AU-6).
5. Step 5: Post-Incident. Document any devices discovered outside the asset inventory and close the gap (CIS 1.1, CIS 1.2). Review network segmentation policy for OT and embedded devices; this vulnerability exposed a default-enabled, unauthenticated UDP service reachable without restriction (NIST AC-4, AC-6). Evaluate whether embedded and IoT devices are included in the vulnerability management program with a defined remediation SLA (CIS 7.1, CIS 7.2). Apply the principle of least privilege to all device-to-network communication paths (NIST AC-6).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership, legal, and (if applicable) physical security management immediately if: UDP/10001 traffic from an unexpected source IP to a GV-I/O Box 4E device is confirmed in logs (indicating active exploitation attempt); any relay output controlling a physical access, safety, or industrial control function is found in an unexpected state; devices are discovered on networks subject to NERC CIP, HIPAA, or critical infrastructure regulatory frameworks where unauthorized physical-system access constitutes a reportable incident.
Recovery Notes	After firmware update or service disablement is confirmed, maintain continuous UDP/10001 monitoring on OT segment firewalls for a minimum of 30 days to detect any attacker persistence or re-exploitation attempts against devices that may have been missed in the initial sweep. Physically audit relay outputs on all GV-I/O Box 4E devices that had confirmed or suspected UDP/10001 contact from unauthorized sources, as successful exploitation could have toggled physical I/O lines controlling doors, alarms, or building systems. Do not treat network-level blocking alone as full eradication — if any device received a payload that achieved code execution prior to containment, assume the device firmware may be modified and require a full factory reset and firmware reinstall before returning to service.
Forensic Artifacts	Full packet capture (PCAP) of UDP/10001 traffic to GV-I/O Box 4E device IPs — the exploit is a single crafted UDP datagram; the payload bytes overflowing the DVRSearch service stack buffer are the primary forensic indicator of exploitation attempt and must be preserved before any ACL blocks drop subsequent traffic. | Device syslog records showing DVRSearch service crashes, watchdog-triggered reboots, or unexpected process terminations, with timestamps correlated to inbound UDP/10001 packets — these establish whether exploitation achieved code execution, not merely a denial-of-service crash. | Firewall and NetFlow session logs for all UDP/10001 conversations involving GV-I/O Box 4E IPs for 30 days preceding discovery — essential for establishing attacker first-contact timestamp, source IP geolocation, and whether scanning or targeted exploitation occurred. | Physical relay output and digital input state audit log or inspection record — GV-I/O Box 4E controls physical I/O lines; any relay in an unexpected state post-exploitation is evidence of physical impact and distinguishes a failed exploit attempt from a successful one with real-world consequences. | Running process list and open file handles from the device diagnostic shell (captured before firmware update or reboot) — if the attacker achieved RCE, a backdoor process, modified binary, or unusual network listener may be present in the embedded Linux environment alongside or replacing the legitimate DVRSearch daemon.

Per-Action IR Details

Step 1: Containment — Immediately identify all GeoVision GV-I/O Box 4E devices on your network using asset inventory records (CIS 1.1). Block inbound and outbound UDP port 10001 at the network perimeter and on internal segmentation boundaries using host-based and server firewalls (CIS 4.4, CIS 4.5, NIST AC-4). Isolate any device that cannot be immediately firewalled to a restricted VLAN with no internet exposure.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), 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 targeted UDP scan from an internal host to enumerate GV-I/O Box 4E devices before firewalling: `nmap -sU -p 10001 --open -oN gvio_discovery.txt`. On each perimeter or distribution firewall/router apply an ACL entry: `deny udp any any eq 10001` (Cisco IOS syntax) or the equivalent `ufw deny proto udp to any port 10001` on Linux-based gateways. For devices that cannot be immediately ACL'd, physically unplug their network uplink and place them on an isolated switch port or unmanaged switch with no uplink until firewalling is confirmed.

Evidence: Before isolating any device suspected of prior compromise, capture volatile network state from adjacent infrastructure: collect NetFlow or firewall session tables showing all UDP/10001 conversations involving GV-I/O Box 4E IPs for the preceding 30 days; export syslog buffers from upstream switches and routers; take a `pcap` of any live UDP/10001 traffic via `tcpdump -i -w gvio_capture_$(date +%Y%m%d%H%M%S).pcap udp port 10001` before applying ACL blocks. These captures are destroyed the moment the firewall rule drops in-flight packets.

Step 2: Detection — Query network flow logs and firewall logs for UDP traffic to port 10001 targeting known GV-I/O Box 4E device IPs. Alert on any external source IP communicating with these devices. Review syslog output from affected devices for unexpected process crashes, reboots, or anomalous relay output activity. Monitor for lateral movement originating from device IP addresses (NIST AU-6, AU-2).

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: If no SIEM is available, use the following CLI pipeline to triage firewall logs on a Linux log aggregator: `grep 'udp.*10001' /var/log/firewall.log | awk '{print $NF, $0}' | sort | uniq -c | sort -rn > gvio_udp10001_hits.txt`. For device syslog, forward GV-I/O Box 4E syslog (if configurable) to `rsyslog` on an analyst workstation and filter: `grep -iE 'crash|reboot|dvrsearch|core|segfault' /var/log/gvio.log`. Deploy a Wireshark capture filter `udp.port == 10001` on a mirror/SPAN port covering the OT segment to catch exploit-shaped oversized DVRSearch UDP payloads in real time. Write a Sigma rule against firewall logs alerting on any source IP outside the expected management subnet communicating with GV-I/O Box 4E device IPs on UDP/10001.

Evidence: The CVE-2026-12485 exploit is delivered as a single crafted UDP packet to port 10001, so the primary detection artifact is that packet itself — capture it before altering network state. Evidence to preserve: (1) Full packet capture of UDP/10001 traffic to device IPs, including payload bytes that overflow the DVRSearch service stack buffer (oversized or malformed DVRSearch protocol fields). (2) Device syslog entries showing DVRSearch service crash or watchdog-triggered reboot immediately following inbound UDP traffic — timestamp correlation to the triggering packet is critical. (3) Any ICMP unreachable or TCP SYN originating from the GV-I/O Box 4E IP after exploitation (indicating post-exploitation callback or lateral movement). (4) Firewall deny/permit logs for UDP/10001 for at minimum 30 days prior to discovery to establish first-contact timeline.

Step 3: Eradication — Check the GeoVision vendor portal for firmware updates addressing CVE-2026-12485, CVE-2026-12846, CVE-2026-12847, and CVE-2026-12848. No specific patch version or advisory URL is confirmed in available source data — contact GeoVision support directly for remediation guidance. If a firmware update is not yet available, disable the DVRSearch service on UDP port 10001 where the device configuration permits, or enforce network-level block as a compensating control (NIST SI-4, CIS 7.1, CIS 7.2).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: If no firmware patch is yet available from GeoVision, use the device's web management interface or serial console (if accessible) to disable or stop the DVRSearch service — document the exact menu path and configuration change for change-management records. Verify the service is no longer listening by re-scanning from an adjacent host: `nmap -sU -p 10001 ` — expected result is `closed` or `filtered`. If service disablement is not possible via the device UI, maintain the UDP/10001 ACL block applied in Step 1 as the sole compensating control and escalate to GeoVision support with explicit reference to CVE-2026-12485 to obtain a remediation timeline in writing.

Evidence: Before applying any firmware update or service-disablement action that modifies the device's running state, preserve the following volatile artifacts: (1) Current firmware version string from the device management interface — screenshot or text export. (2) Running process list if the device exposes a diagnostic shell (e.g., via Telnet or serial console): `ps aux` or equivalent embedded Linux command, capturing whether the DVRSearch daemon (`dvrsearch` or equivalent binary name) is active. (3) Network connection state from the device if accessible: `netstat -anup` output showing UDP/10001 listener. (4) Any crash dumps or core files in `/tmp`, `/var/log`, or device-specific log directories

that the DVRSearch service may have written after a prior exploitation attempt — these are destroyed on reboot or firmware flash.

Step 4: Recovery — After applying firmware updates or compensating controls, verify UDP port 10001 is no longer reachable from unauthorized segments using a port scanner run from an external and internal vantage point. Confirm device relay outputs and input states are operating as expected and have not been manipulated. Re-enable monitored network access only after verification. Retain logs from the isolation period for post-incident review (NIST AU-11, AU-6).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), CIS 8.2 (Collect Audit Logs)

Compensating: Perform verification scans from two network positions — once from outside the OT VLAN (simulating lateral attacker access) and once from inside the authorized management subnet: `nmap -sU -p 10001 --reason ` from each vantage. Confirm the result is `filtered` (ACL block active) or `closed` (service disabled). For relay output integrity, if the device has no audit log for physical output state, physically inspect each relay output terminal and compare against the expected state documented in the device's baseline configuration record. Archive all firewall, syslog, and packet capture logs from the isolation period to write-once storage (e.g., WORM-configured S3 bucket, optical media, or an append-only NFS share) before re-enabling network access.

Evidence: Before re-enabling full network access to any GV-I/O Box 4E device, document the post-remediation baseline: (1) Nmap scan output confirming UDP/10001 is no longer reachable from each test vantage — save as timestamped text file. (2) Current firmware version string post-update to confirm the correct patch was applied. (3) Device relay and I/O state audit — if any relay output is in an unexpected state (e.g., a door lock actuator left in an open/active state by a successful exploit), treat this as evidence of physical impact and escalate immediately; document the pre-correction state before resetting. (4) Archived syslog from the isolation period demonstrating no DVRSearch crash events occurred during the remediation window.

Step 5: Post-Incident — Document any devices discovered outside the asset inventory and close the gap (CIS 1.1, CIS 1.2). Review network segmentation policy for OT and embedded devices — this vulnerability exposed a default-enabled, unauthenticated UDP service reachable without restriction (NIST AC-4, AC-6). Evaluate whether embedded and IoT devices are included in the vulnerability management program with a defined remediation SLA (CIS 7.1, CIS 7.2). Apply the principle of least privilege to all device-to-network communication paths (NIST AC-6).

NIST Phase: Post Incident

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 1.2 (Address Unauthorized Assets), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For asset inventory gap closure, run a recurring weekly UDP scan of all internal subnets for port 10001 using a scheduled cron job: `0 2 * * 1 nmap -sU -p 10001 -oN /var/log/gvio_sweep_$(date +%Y%m%d).txt` — any new host responding indicates an undiscovered GV-I/O Box 4E or a new device using the same port. Add GeoVision GV-I/O Box 4E to the vulnerability management asset class with a tag `embedded-OT` and define a 72-hour critical-patch SLA to match the CVSS 10.0 severity. For segmentation policy, document a standing rule that no OT or embedded device with a default-enabled unauthenticated UDP service is permitted to have an ACL path to internet-routable addresses or corporate IT segments without explicit documented justification.

Evidence: Post-incident evidence collection for lessons-learned and regulatory documentation: (1) Complete asset inventory delta report — list of GV-I/O Box 4E devices found during incident response that were absent from the pre-incident inventory. (2) Timeline reconstruction from firewall and syslog data establishing first observed UDP/10001 contact with each device, to support breach notification window calculations if exploitation is confirmed. (3) Final disposition record for each device: firmware version applied, service state, network segment, and responsible owner. (4) Written confirmation from GeoVision (email or support ticket) of patch version that addresses CVE-2026-12485,

CVE-2026-12846, CVE-2026-12847, and CVE-2026-12848 — retain for audit evidence that remediation was vendor-validated.

Detection Guidance

Monitor for UDP traffic directed to port 10001 on any GeoVision GV-I/O Box 4E device IP addresses. In firewall or network flow logs, filter on proto=UDP and dport=10001; alert on any source outside approved management subnets. Packet payloads at or near the maximum input size of 1460 bytes are a strong indicator of exploitation attempts, as legitimate DVRSearch messages are typically much smaller; capture and inspect these where possible. On the device side, look for unexpected reboots, service crashes, or relay state changes not correlated with authorized control actions. If SIEM ingestion of device syslog is available, create a rule for repeated UDP connections from a single external source to port 10001 within a short time window. Behavioral indicators include: device responding abnormally after a UDP burst, new outbound connections from device IPs to unknown external hosts post-exploitation (indicating RCE achieved), or physical relay outputs toggling without corresponding authorized commands. MITRE ATT&CK techniques T1190 (Exploit Public-Facing Application) and T1499.004 (Application or System Exploitation) apply. No confirmed public IOCs (IPs, hashes, domains) are associated with active exploitation in the provided source data.

Framework Mappings

MITRE-ATTACK

- **T1499.004** — Application or System Exploitation
- **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

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1499.004	Application or System Exploitation	Impact
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-12485	T1
(consolidated)	https://nvd.nist.gov/vuln/detail/CVE-2026-12846	T1
(consolidated)	https://nvd.nist.gov/vuln/detail/CVE-2026-12847	T1
(consolidated)	https://nvd.nist.gov/vuln/detail/CVE-2026-12848	T1
CVE-2026-12485 in GV-IO Box 4E	https://vuldb.com/cve/CVE-2026-12485	T3

Generated 2026-06-27 06:09 UTC by TJS Security Command Center