INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-17 08:05 UTC

CVE-2026-54413: driftregion iso14229 through 0.9.0 contains an integer underflow and downstream out-of-bounds read i...

CVE VULNERABILITY | HIGH | CVSS 8.2

SCC Item ID	SCC-CVE-2026-0318
Type	CVE Vulnerability
CVE ID	CVE-2026-54413
Severity	HIGH
CVSS Base Score	8.2
EPSS Score	0.0046 (36th percentile)
Affected Products	driftregion iso14229 through version 0.9.0
Published	2026-06-14T18:17:20.943
Discovery Source	Nvd

Executive Summary

A memory corruption flaw in the open-source iso14229 UDS diagnostic library allows an unauthenticated attacker to crash automotive ECUs, industrial controllers, and IoT devices, or read sensitive memory contents, by sending a single malformed diagnostic request. The vulnerability requires no prior authentication and is reachable over standard automotive transport layers including CAN bus, OBD-II, and DoIP. Organizations embedding iso14229 version 0.9.0 or earlier in vehicle or industrial firmware face potential operational disruption, safety-adjacent risk, and exposure of in-memory diagnostic data.

Technical Analysis

CVE-2026-54413 affects driftregion iso14229 through version 0.9.0. The flaw resides in Handle_0x27_SecurityAccess() in iso14229.c and involves two chained weaknesses: CWE-191 (integer underflow) and CWE-125 (out-of-bounds read). The handler reads SecurityAccess subFunction from recv_buf[1] without first verifying recv_len is at least 2. When recv_len equals 1, the expression (uint16_t)(recv_len - UDS_0X27_REQ_BASE_LEN) underflows to 65535. That value is passed directly to the SecAccessValidateKey or SecAccessRequestSeed application callback, which typically iterates or copies up to 65535 bytes from a 4 KB receive buffer, producing an out-of-bounds read. The trigger is a single-byte 0x27 SecurityAccess request sent after any prior well-formed 0x27 message. The handler is reachable without

authentication in the default diagnostic session over CAN bus, OBD-II, ISO-TP, and DoIP transports. All other sub-function handlers in the library perform explicit recv_len lower-bound checks; Handle_0x27_SecurityAccess is the sole outlier. MITRE ATT&CK mappings: T1190 (Exploit Public-Facing Application), T1005 (Data from Local System), T1499.004 (Application or System Exploitation). CVSS base score: 8.2 (High). EPSS: 0.00459 (36th percentile). Not currently listed in CISA KEV.

Action Checklist

1. Step 1: Containment. Identify all firmware builds, ECU images, and embedded device deployments that include driftregion iso14229 version 0.9.0 or earlier. Implement network- or transport-layer access controls to restrict diagnostic session traffic where possible: disable or firewall DoIP endpoints, limit OBD-II port physical access, and block unauthenticated CAN bus diagnostic frames at gateway ECUs until patched firmware is available. Reference NIST AC-4 (Information Flow Enforcement) for transport-layer access control segmentation.
2. Step 2: Detection. Audit firmware build manifests, software component inventories, and SBOM records for iso14229 as a dependency. Per CIS 2.1 (Establish and Maintain a Software Inventory), confirm whether iso14229 is present and at what version. On network-connected devices exposing DoIP, monitor for single-byte 0x27 UDS service requests (hex: 27) arriving without a preceding multi-byte SecurityAccess sequence. Log any ECU crash or unexpected reset events correlated with diagnostic session activity on CAN/OBD-II/DoIP channels. No published IOC hashes or IP indicators are available at this time.
3. Step 3: Eradication. Apply a vendor- or maintainer-supplied patch to Handle_0x27_SecurityAccess() that adds an explicit recv_len lower-bound check (recv_len >= 2) before reading recv_buf[1] or computing key-data length. If no patch is yet released by the driftregion iso14229 project, apply the workaround of adding the bounds check locally and rebuilding firmware. Follow CIS 7.4 (Perform Automated Application Patch Management) for tracking patch deployment across all affected device classes. Validate the fix eliminates the underflow path before reflashing production units.
4. Step 4: Recovery. After deploying patched firmware, conduct functional testing of the UDS SecurityAccess service to confirm normal diagnostic session behavior is restored. Monitor ECU telemetry and crash/reset logs for any recurrence. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) by reviewing diagnostic session logs for anomalous single-byte 0x27 requests in the period prior to remediation to determine whether exploitation was attempted.
5. Step 5: Post-Incident. Review SBOM practices for all embedded firmware products to ensure third-party C libraries are tracked at the function level, not just the package level (CIS 2.1). Evaluate whether the absence of a recv_len bounds check in this handler was caught during code review; if not, introduce static analysis rules targeting CWE-191 and CWE-125 in the CI/CD pipeline. Assess whether NIST SI-4 monitoring coverage extends to automotive and OT diagnostic transports. Document a control gap if UDS-layer diagnostic traffic is not currently included in network monitoring scope.

Detection Guidance

Primary detection method is SBOM and software inventory review. Query build manifests, package lock files, and component databases for 'iso14229' or 'driftregion/iso14229' at any version at or below 0.9.0 (CIS 2.1). For network-connected devices, monitor DoIP traffic (UDP/TCP port 13400) for UDS service 0x27 frames with a

data length of exactly 1 byte following any prior 0x27 exchange. On CAN bus environments, log PGN/arbitration IDs associated with UDS diagnostic sessions and flag single-byte service 0x27 requests. ECU crash counters or unexpected resets correlated temporally with diagnostic session activity are a behavioral indicator of exploitation attempts. No confirmed IOC hashes, IP addresses, or domain indicators are associated with this CVE at this time. Per NIST AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting), ensure diagnostic session events are captured in audit logs with timestamps sufficient to reconstruct request sequences.

Framework Mappings

MITRE-ATTACK

- **T1005** — Data from Local System
- **T1190** — Exploit Public-Facing Application
- **T1499.004** — Application or System Exploitation

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

CIS-V8

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

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1005	Data from Local System	Collection
T1190	Exploit Public-Facing Application	Initial-Access
T1499.004	Application or System Exploitation	Impact

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-54413	T1

Source	URL	Tier
CVE-2026-54413 - Vulnerability Details - OpenCVE	https://app.opencve.io/cve/CVE-2026-54413	T3
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1

Generated 2026-06-17 08:05 UTC by TJS Security Command Center