INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-02 06:33 UTC

CVE-2026-10110: A vulnerability was detected in code-projects Student Details Management System 1.0. This affects an...

CVE VULNERABILITY | HIGH | CVSS 7.3

SCC Item ID	SCC-CVE-2026-0254
Type	CVE Vulnerability
CVE ID	CVE-2026-10110
Severity	HIGH
CVSS Base Score	7.3
EPSS Score	0.0003 (9th percentile)
Affected Products	code-projects Student Details Management System 1.0
Published	2026-05-30T07:16:27.813
Discovery Source	Nvd

Executive Summary

CVE-2026-10110 is a high-severity SQL injection vulnerability in code-projects Student Details Management System 1.0, a small-scale academic web application. An unauthenticated remote attacker can manipulate the 'roll' parameter in /index.php to extract, modify, or delete student records from the underlying database. A public exploit is available, lowering the barrier for opportunistic attackers; however, the product's narrow deployment base limits broad organizational exposure.

Technical Analysis

CVE-2026-10110 affects code-projects Student Details Management System 1.0. The vulnerability is a classic SQL injection (CWE-89) via improper input neutralization (CWE-74) in the 'roll' GET/POST parameter handled by /index.php. No authentication is required. An attacker can craft malicious SQL syntax in the 'roll' argument to manipulate backend database queries, enabling data extraction, modification, or deletion. MITRE ATT&CK technique T1190 (Exploit Public-Facing Application) applies. CVSS base score is 7.3 (High). EPSS score is 0.0003 (9th percentile), indicating low observed exploitation activity at this time despite a public exploit being available. No CISA KEV listing as of configuration date. No vendor patch has been confirmed in available source data. Primary reference: NVD (https://nvd.nist.gov/vuln/detail/CVE-2026-10110).

Action Checklist

1. Step 1: Containment. Immediately restrict public internet access to any instance of code-projects Student Details Management System 1.0. If internet-facing, place it behind a WAF or take it offline until remediation is confirmed. Per NIST AC-17, document and enforce access controls for remote access to sensitive systems.
2. Step 2a: Detection, Query Patterns. Query web server access logs for requests to /index.php containing SQL metacharacters in the 'roll' parameter: single quotes ('), double dashes (--), UNION, SELECT, or OR 1=1 patterns.
3. Step 2b: Detection, Logging Setup. Enable AU-2 event logging on the web server and database layer if not already active. Enable database query logging per your database engine documentation (MySQL: general_log; PostgreSQL: log_statement; MSSQL: Query Store or SQL Server Agent). Reference CIS 8.2.
4. Step 2c: Detection, Log Review. Review database query logs for anomalous SELECT or UNION-based patterns originating from the application account.
5. Step 3: Eradication. No official vendor patch has been confirmed in available source data. Apply input validation and parameterized queries to the 'roll' parameter as an immediate code-level fix, consistent with OWASP SQL Injection Prevention guidance. If the application cannot be patched, implement WAF rules blocking SQL injection patterns against /index.php per CIS 4.4/4.5. Document any exception per CIS 7.2 remediation process requirements.
6. Step 4: Recovery. After applying input validation or WAF controls, conduct a database integrity review to determine whether unauthorized queries were executed prior to remediation. Validate that /index.php no longer accepts SQL metacharacters in the 'roll' parameter via manual or automated testing. Monitor database access logs for continued anomalous activity per AU-6 audit record review requirements. Confirm logging is functioning per AU-5.
7. Step 5: Post-Incident. Review whether this application was inventoried per CIS 2.1 (software inventory) and CIS 1.1 (asset inventory). If not inventoried, this incident reveals an asset visibility gap. Evaluate whether AC-3 (access enforcement) and AC-6 (least privilege) apply to the application's database account, the account should have only minimum required permissions. Document control gaps in your vulnerability management process per CIS 7.1.

Detection Guidance

Monitor web server access logs for requests to /index.php where the 'roll' parameter contains SQL injection patterns: single quotes ('), double dashes (--), UNION SELECT strings, OR 1=1 sequences, or encoded equivalents (%27, %2D%2D). At the database layer, enable and review query logs for unexpected UNION, DROP, INSERT, or UPDATE statements originating from the application's database account. Query log enabling steps vary by database engine, for MySQL, enable general_log; for PostgreSQL, enable log_statement; for MSSQL, use Query Store or SQL Server Agent. Consult your database vendor documentation for specifics. A WAF or IDS with OWASP CRS rules (SQLi category) will surface matching requests. No confirmed IOCs (IPs, domains, hashes) are available for this CVE at this time; detection relies on behavioral and pattern-based indicators. Reference NIST SI-4 for system monitoring requirements and AU-12 for audit record generation at the application and database tiers. D3FEND countermeasure D3-SFA (System File Analysis) applies for monitoring application and database logs for tampering or anomalous query patterns.

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-10** — Information Input Validation
- **SI-4** — System Monitoring
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **8.2** — Collect Audit Logs

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored
- **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

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-10110	T1

Source	URL	Tier
CVE-2026-10110 | Tenable®	https://www.tenable.com/cve/CVE-2026-10110	T3
CVE-2026-1010 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-1010	T1
CVE-2026-10110 - code-projects Student Details Management ...	https://cvefeed.io/vuln/detail/CVE-2026-10110	T3
A vulnerability was detected in code-projects Student... · CVE-2026 ...	https://github.com/advisories/GHSA-gv5v-x8h4-8rmj	T3

Generated 2026-06-02 06:33 UTC by TJS Security Command Center