# CVE Detail – CVE-2024-50672

A NoSQL injection vulnerability in Adapt Learning Adapt Authoring Tool <= 0.11.3 allows unauthenticated attackers to reset user and administrator account passwords via the "Reset password" feature. The vulnerability occurs due to insufficient validation of user input, which is used as a query in Mongoose's find() function. This makes it possible for attackers to perform a full takeover of the administrator account. Attackers can then use the newly gained administrative privileges to upload a custom plugin to perform remote code execution (RCE) on the server hosting the web application.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.27875

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

## CAPEC(s)

* CAPEC-108: Command Line Execution through SQL Injection
* CAPEC-109: Object Relational Mapping Injection
* CAPEC-110: SQL Injection through SOAP Parameter Tampering
* CAPEC-470: Expanding Control over the Operating System from the Database
* CAPEC-66: SQL Injection
* CAPEC-7: Blind SQL Injection