# CVE Detail – CVE-2023-32530

Vulnerable modules of Trend Micro Apex Central (on-premise) contain vulnerabilities which would allow authenticated users to perform a SQL injection that could lead to remote code execution.

Please note: an attacker must first obtain authentication on the target system in order to exploit these vulnerabilities.

This is similar to, but not identical to CVE-2023-32529.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.86522

## CVSS Scoring

CVSS v3.1 Score: 8.8

Severity: HIGH

## 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

## Affected Products

* cpe:2.3:a:trendmicro:apex\_central:2019:-:\*:\*:\*:windows:\*:\*