# CVE Detail – CVE-2021-42258

BQE BillQuick Web Suite 2018 through 2021 before 22.0.9.1 allows SQL injection for unauthenticated remote code execution, as exploited in the wild in October 2021 for ransomware installation. SQL injection can, for example, use the txtID (aka username) parameter. Successful exploitation can include the ability to execute arbitrary code as MSSQLSERVER$ via xp\_cmdshell.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.99857

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## CISA KEV

KEV is present

## 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:bqe:billquick\_web\_suite:\*:\*:\*:\*:\*:\*:\*:\*