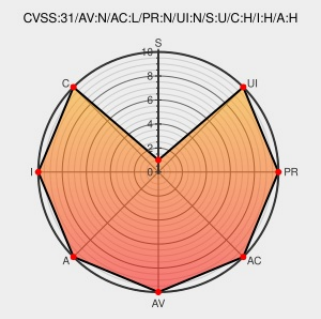
CVE-2021-42258

Published on: 10/22/2021 12:00:00 AM UTC

Last Modified on: 10/28/2021 08:34:00 PM UTC

CVE-2021-42258

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Billquick Web Suite from Bqe contain the following vulnerability:

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.

CVE-2021-42258 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Threat Advisory: Hackers Are Exploiting a Vulnerability in Popular Billing Software to Deploy Ransomware	www.huntress.com text/html	MISC www.huntress.com/blog/threat-advisory-hackers-are-exploiting-a-vulnerability-in-popular-billing-software-to-

deploy-ransomware

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

730246 BQE BillQuick Web Suite SQL Injection Vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bqe	Billquick Web Suite	All	All	All	All

cpe:2.3:a:bqe:billquick_web_suite:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-42258 : BQE BillQuick Web Suite 2018 through 2021 before 22.0.9.1 allows SQL injection for unauthenticated… twitter.com/i/web/status/1…	2021-10-22 22:03:39
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-42258 Description: BQE BillQuick Web Suite 2018 through 2021 before 22.… twitter.com/i/web/status/1…	2021-10-22 23:00:14
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-42258 Description: BQE BillQuick Web Suite 2018 through 2021 before 22.… twitter.com/i/web/status/1…	2021-10-23 11:30:09

← Previous ID

Next ID→