Hive Pro

THREAT ADVISORY

BillQuick Web Suite's severe vulnerability may affect 400K users

TA202143

Threat Level RED

Publish Date – Oct 26, 2021

Multiple versions of BillQuick Web Suite have been found to have a critical vulnerability. A hacker was able to get initial access to a US engineering company by exploiting this serious vulnerability (CVE-2021-42258). It also infected the victim's network with ransomware. This vulnerability can be addressed by upgrading BillQuick's BQE Software to version 22.0.9.1. Eight more vulnerabilities(CVE-2021-42344, CVE-2021-42345, CVE-2021-42346, CVE-2021-42571, CVE-2021-42572, CVE-2021-42573, CVE-2021-42741, CVE-2021-42742) have been uncovered, but no formal patch has been released.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-42258	BillQuick Web Suite versions up to 2021 22.0.9	cpe:2.3:a:bqe:billquick_web_suite:2021_22.0:*:*:*:*:*:*:*, cpe:2.3:a:bqe:billquick_web_suite:2021_22.0.1:*:*:*:*:*:*:*, cpe:2.3:a:bqe:billquick_web_suite:2021_22.0.2:*:*:*:*:*:*:*, cpe:2.3:a:bqe:billquick_web_suite:2021_22.0.3:*:*:*:*:*:*:*, cpe:2.3:a:bqe:billquick_web_suite:2021_22.0.4:*:*:*:*:*:*:* , cpe:2.3:a:bqe:billquick_web_suite:2021_22.0.5:*:*:*:*:*:*:* , cpe:2.3:a:bqe:billquick_web_suite:2021_22.0.6:*:*:*:*:*:*:*, cpe:2.3:a:bqe:billquick_web_suite:2021_22.0.7:*:*:*:*:*:*:* , cpe:2.3:a:bqe:billquick_web_suite:2021_22.0.8:*:*:*:*:*:*:* , cpe:2.3:a:bqe:billquick_web_suite:2021_22.0.9:*:*:*:*:*:*:*	BillQuick Web Suite SQL injection	CWE-89

References

https://www.huntress.com/blog/threat-advisory-hackers-are-exploiting-a-vulnerability-in-popular-billing-software-to-deploy-ransomware
https://www.bleepingcomputer.com/news/security/hackers-used-billing-software-zero-day-to-deploy-ransomware/