# [AIT-SA-20210215-02] CVE-2020-24913: QCubed SQL Injection

*From*: sec-advisory <sec-advisory () ait ac at>
*Date*: Fri, 12 Mar 2021 10:47:29 +0000

```
QCubed SQL Injection
====================

| Identifier: | AIT-SA-20210215-02 |
| Target: | QCubed Framework |
| Vendor: | QCubed |
| Version: | all versions including 3.1.1 |
| CVE: | CVE-2020-24913 |
| Accessibility: | Remote |
| Severity: | Critical |
| Author: | Wolfgang Hotwagner (AIT Austrian Institute of Technology) |

SUMMARY
=======
QCubed is a PHP Model-View-Controller Rappid Application Development framework. (https://github.com/qcubed/qcubed)

VULNERABILITY DESCRIPTION
=========================
A SQL injection vulnerability in qcubed (all versions including 3.1.1)  in profile.php via the strQuery parameter
allows an unauthenticated  attacker to access the database by injecting SQL code via a crafted POST  request.  The
strQuery parameter of the serialized array in profile.php  could lead to a sql-injection. This parameter is used by
the
 PrintExplainStatement which simply concats "EXPLAIN ." with this  parameter:

public function ExplainStatement($sql) {
     return $this->Query("EXPLAIN " . $sql);
}


This query will be executed unfiltered.

We were able to write proof-of concept exploit for mysql and postgres.  Unfortunately with mysql we were not able to
use a  stacked-queries-payload and we had to exploit this vulnerability with a  timebased approach.


VULNERABLE VERSIONS
===================
All versions including 3.1.1 are affected.


TESTED VERSIONS
===============
QCubed 3.1.1

IMPACT
======
An unauthenticated attacker could  access the database remotely. In  worst case scenarios an attacker might be able to
execute code on the  remote machine

MITIGATION
==========

A patch was delivered by QCubed that allows to disable the profile-functionality(
https://github.com/qcubed/qcubed/pull/1320/files ).

VENDOR CONTACT TIMELINE
=======================

| 2020-04-19 | Contacting the vendor |
| 2020-04-19 | Vendor replied |
| 2020-05-01 | Vendor released a patch at Github |
| 2021-02-15 | Public disclosure |

ADVISORY URL
============

[https://www.ait.ac.at/ait-sa-20210215-02-unauthenticated-sql-injection-qcubed] (https://www.ait.ac.at/ait-sa-20210215-
02-unauthenticated-sql-injection-qcubed)


_____
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

By Date By Thread

**Current thread:**

**[AIT-SA-20210215-02] CVE-2020-24913: QCubed SQL Injection** *sec-advisory (Mar 12)*

Site Search

**Nmap Security Scanner**
Ref Guide
Install Guide
Docs
Download
Nmap OEM

**Npcap packet capture**
User's Guide
API docs
Download
Npcap OEM

**Security Lists**
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

**Security Tools**
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

**About**
About/Contact
Privacy
Advertising
Nmap Public Source License