[AIT-SA-20210215-01] CVE-2020-24914: QCubed PHP Object Injection

From: sec-advisory <sec-advisory () ait ac at>
Date: Fri, 12 Mar 2021 10:46:40 +0000

```
QCubed PHP Object Injection
===========================

| Identifier: | AIT-SA-20210215-01 |
| Target: | QCubed Framework |
| Vendor: | QCubed |
| Version: | all versions including 3.1.1 |
| CVE: | CVE-2020-24914 |
| 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 PHP object injection bug in profile.php in qcubed (all versions including 3.1.1) unserializes the untrusted data of
the POST-variable "strProfileData" and allows an unauthenticated attacker to execute code via a crafted POST request.

qcubed/assets/php/profile.php:
<?php
    require_once('./qcubed.inc.php');

    //Exit gracefully if called directly or profiling data is missing.
    if ( !isset($_POST['intDatabaseIndex']) && !isset($_POST['strProfileData']) && !isset($_POST['strReferrer']) )
        exit('Nothing to profile. No Database Profiling data recived.');

    if ( !isset($_POST['intDatabaseIndex']) || !isset($_POST['strProfileData']) || !isset($_POST['strReferrer']) )
        throw new Exception('Database Profiling data appears to have been corrupted.');

    $intDatabaseIndex = intval($_POST['intDatabaseIndex']);
    $strReferrer = QApplication::HtmlEntities($_POST['strReferrer']);

    $objProfileArray = unserialize(base64_decode($_POST['strProfileData']));  //<-VULNERABLE CODE
    $objProfileArray = QType::Cast($objProfileArray, QType::ArrayType);


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


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

IMPACT
======
An unauthenticated attacker could  execute code remotely.

MITIGATION
==========
A patch was delivered by QCubed that allows to disable the profile-functionality.

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-20210215-01-unauthenticated-remote-code-execution-qcubed](https://www.ait.ac.at/ait-sa-20210215-01-unauthenticated-remote-code-execution-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-20210215-01] CVE-2020-24914: QCubed PHP Object Injection ***sec-advisory (Mar 12)***