QCubed PHP Object Injection (CVE-2020-24914)

2 March 2021

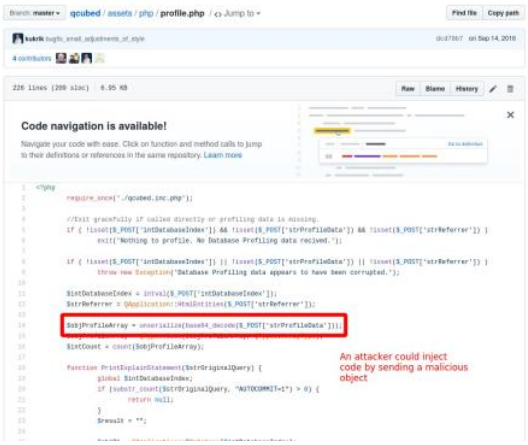
Identifier:	AIT-SA-20210215-01
Target:	QCubed Framework
Vendor:	QCubed
Version:	all versions including 3.1.1
CVE:	CVE-2020-24914
Accessibility:	Remote
Severity:	Critical
Author:	Wolfgang Hotwagner (AIT Austrian Institute of Technology)

Summary

QCubed is a PHP Model-View-Controller Rappid Application Development framework.

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.



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

[PHP Programming Web Security CVE]

My name is Wolfgang Hotwagner. I am a Linux and Information Security enthusiast. This blog is about my journey through Computer Science.

Tag Cloud

Ruby Virtualization openssl Proxy Blog Desktop News xmas Programming apache Database Fun Ansible Web CVE External Firewall HackADay Kernel PHP Mail Network LVM Software-Raid Certification Downloads CLI Crypto Hardware Raspberry Perl Email vim Docker One-Liner Bash TerminalEmulator Sysadmin Shell Linux Postgresql Zsh Btrfs Suricata Backup Toscom Multimedia Open-Source Security C Debian Mathematics Puppet logrotate Tricks Nagios git Anniversary

Recent Posts

- BSidesVienna 2022: Logrotten.
- SexyPolling SQL Injection
- Seventh Anniversary
- ForkCMS PHP Object Injection (CVE-2020-24036)
- QCubed Cross Site Scripting (CVE-2020-24912)
- QCubed SQL Injection (CVE-2020-24913)
- QCubed PHP Object Injection (CVE-2020-24914)
- Pimp my shell
- Refurbished Blog
- How to build a music-box for children

Except where otherwise noted, content on this site is licensed under a Creative Commons Attribution 3.0 Unported License.
Copyright 2015-present Hoti