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)

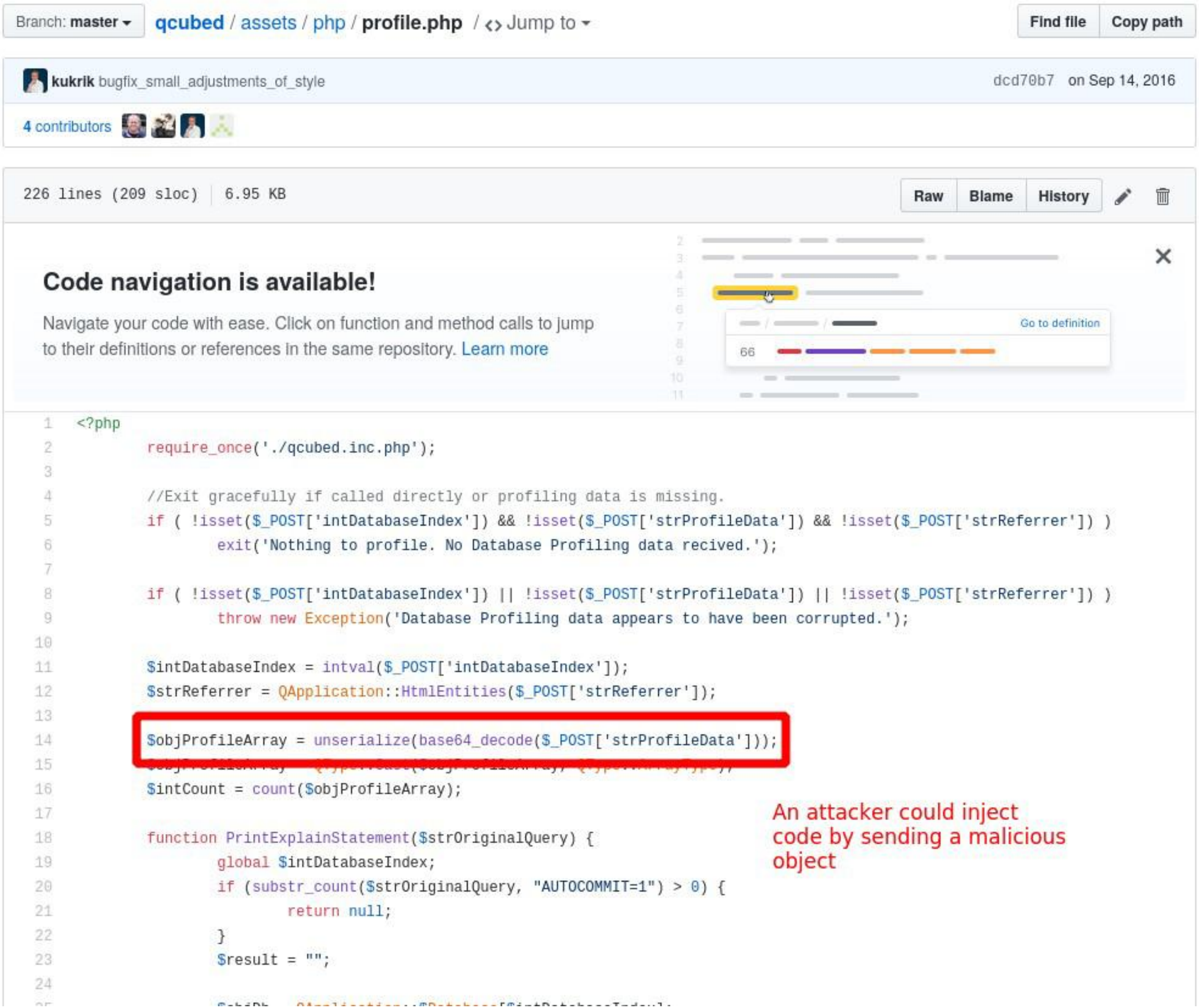
VULNERABILITY DESCRIPTION

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.

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

☎ Anrufen (tel:0043505500) ✉ E-Mail 📍 Standorte (/ueber-das-ait/standorte-und-tochterunternehmen)


Branch: master
qcubed / assets / php / profile.php / <> Jump to
Find file
Copy path
kukrik bugfix_small_adjustments_of_style
dcd70b7 on Sep 14, 2016
4 contributors
226 lines (209 sloc) | 6.95 KB
Raw
Blame
History
Go to definition

Code navigation is available!

Navigate your code with ease. Click on function and method calls to jump to their definitions or references in the same repository. Learn more

```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']));
	$objProfileArray = QType::Cast($objProfileArray, QType::ArrayType);
	$intCount = count($objProfileArray);

	function PrintExplainStatement($strOriginalQuery) {
		global $intDatabaseIndex;
		if (substr_count($strOriginalQuery, "AUTOCOMMIT=1") > 0) {
			return null;
		}
		$result = "";

		$objDb = QApplication::$Database[$intDatabaseIndex];
```

An attacker could inject code by sending a malicious object

(/fileadmin/mc/digital_safety_security/images/CVE.jpg)

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. (https://github.com/qcubed/qcubed/pull/1320/files)

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)

WOLFGANG HOTWAGNER

Research Engineer /
Security & Communication Technologies

☎ +43 664 88335483 (tel:+43 664 8833 5483)

📠 +43 50550-4150

✉ wolfgang.hotwagner(at)ait.ac.at (mailto:wolfgang.hotwagner@ait.ac.at)

(/)

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH

Giefinggasse 4
1210 Vienna
Austria

office@ait.ac.at (mailto:office@ait.ac.at)
+43 50550-0 (tel:+4350550-0)

Impressum (/impressum)

NAVIGATION

- Über das AIT (/ueber-das-ait)
- Themen (/themen)
- Lösungen (/loesungen)
- Publikationen (/publikationen)
- Media (/media)
- News & Events (/news-events)
- Karriere (/karriere)
- Kontakt (/kontakt)

FOLLOW US

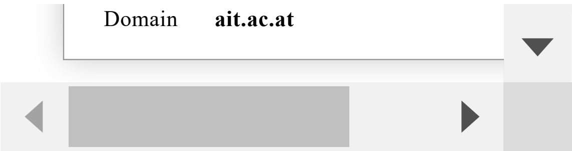
- YouTube (https://www.youtube.com/user/AITTomorrowToday)
- Twitter (https://twitter.com/aittomorrow2day)
- Facebook (https://www.facebook.com/AITtomorrow2day/)
- LinkedIn (https://www.linkedin.com/company/austrian-institute-of-technology/)
- ResearchGate (https://www.researchgate.net/institution/AIT-Austrian-Institute-of-Technology)
- AIT Newsletter (/news-events/ait-newsletter)
- AIT-Blog (https://www.ait.ac.at/blog)
- AIT-Podcast (https://open.spotify.com/show/4ZAdiTs8KcJXH3c8NfQeES)
- AIT-Podcast (https://soundcloud.com/user-378778548)

LINKS

- Sitemap (/sitemap)
- Standorte und Tochterunternehmen (/ueber-das-ait/standorte-und-tochterunternehmen)
- AGB (/agb)
- Zertifizierungen (/ueber-das-ait/zertifizierungen)
- Akkreditierung (/ueber-das-ait/akkreditierung)
- Disclaimer & Data Protection (/disclaimer-data-protection)
- Barrierefreiheit (/barrierefreiheit)
- Incident Reporting (/incident-reporting)
- Covid-19 Schutzmaßnahmen (/fileadmin/user_upload/Infoblatt_COVID-19_Besuchende_Extern.pdf)

WACA Web Accessibility Certificate Austria
www.waca.at
zertifiziert **09/2021**

☎ Anrufen (tel:0043505500) ✉ E-Mail Standorte (/ueber-das-ait/standorte-und-tochterunternehmen)



Domain **ait.ac.at**