



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)



[KIS-2020-11] qdPM <= 9.1 (executeExport) PHP Object Injection Vulnerability

From: Egidio Romano <n0b0d13s () gmail com>

Date: Wed, 30 Dec 2020 22:19:30 +0100

qdPM <= 9.1 (executeExport) PHP Object Injection Vulnerability

[~] Software Link:

<http://qdpn.net>

[~] Affected Versions:

Version 9.1 and prior versions.

[~] Vulnerability Description:

The vulnerability is located in the
/core/apps/qdPM/modules/timeReport/actions.class.php
script, specifically within the timeReportActions::executeExport() method:

```
295. public function executeExport(sfWebRequest $request)
296. {
297.     $separator = "\t";
298.     $format = $request->getParameter('format');
299.     $filename = $request->getParameter('filename');
300.
301.     $export = unserialize($request->getParameter('export'));
```

User input passed through the "export" request parameter is not properly sanitized before being used in a call to the unserialize() function at line 301. This can be exploited by malicious users to inject arbitrary PHP objects into the application scope, allowing them to carry out a variety of attacks, such as executing arbitrary OS commands.

[~] Proof of Concept:

<http://karmainsecurity.com/pocs/CVE-2020-26165>

[~] Solution:

No official solution is currently available.

[~] Disclosure Timeline:

[29/02/2020] - Vendor notified
[08/04/2020] - No response, vendor contacted again
[09/04/2020] - Vendor replies they will fix the vulnerability in a summer release
[30/09/2020] - Summer is gone and a new version hasn't been released, vendor contacted again
[30/09/2020] - Vendor replies they're working on version 10, and should be ready in this year
[30/09/2020] - CVE number requested and assigned
[02/12/2020] - Vendor informed about public disclosure by the end of the year
[30/12/2020] - Public disclosure

[~] CVE Reference:

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2020-26165 to this vulnerability.

[~] Credits:

Vulnerability discovered by Egidio Romano.

[~] Original Advisory:

<http://karmainsecurity.com/KIS-2020-11>

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:

[KIS-2020-11] qdPM <= 9.1 (executeExport) PHP Object Injection Vulnerability *Egidio Romano (Jan 03)*



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

