Unveiling the Unseen

A Responsible Approach to Web Vulnerability Disclosure

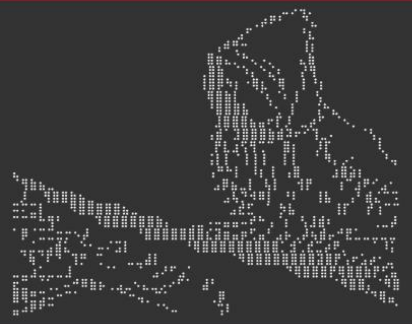
ACCESS42 Cybersecurity

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

ACCESS42 Cybersecurity

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

ACCESS42 Cybersecurity

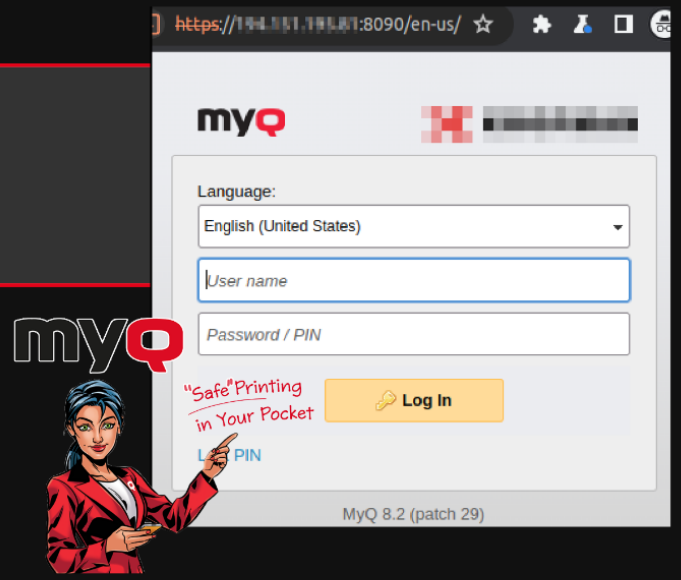
Agenda

- 🧩 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
```



Default Admin Credentials

*this happens more often than you think

4.3. Passwords

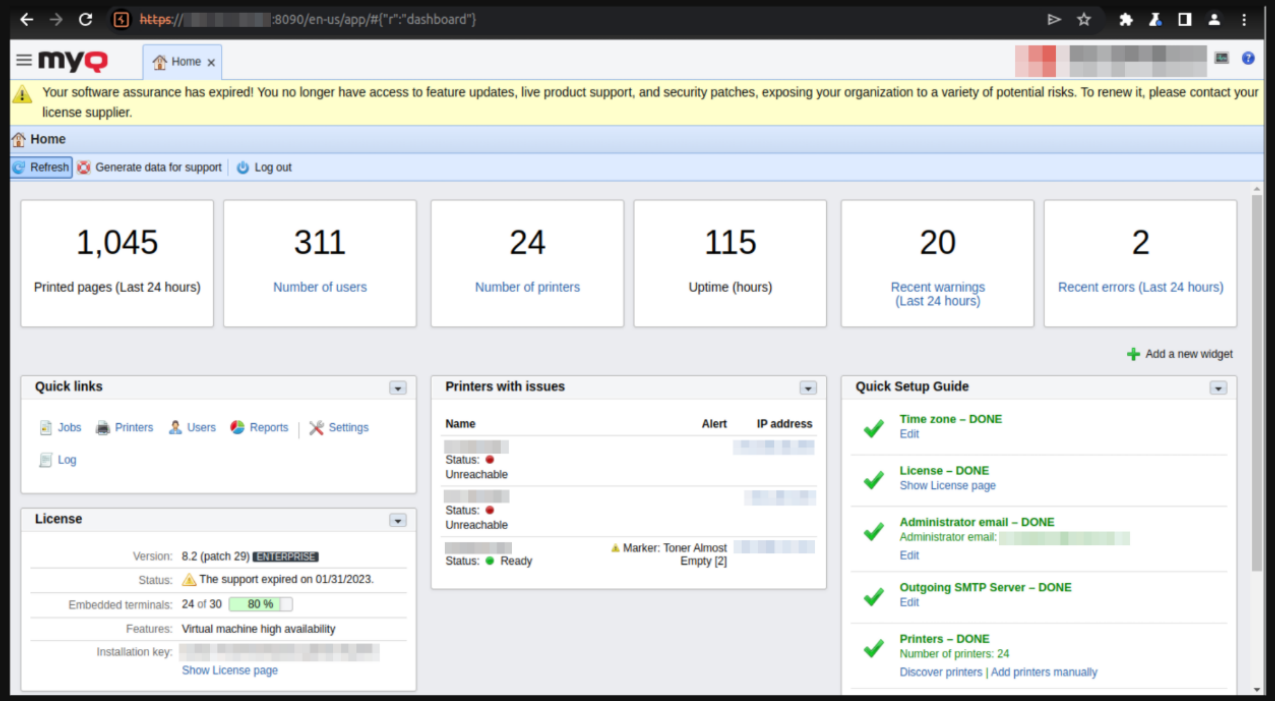
On the **Home** tab and on the **Settings** tab of the MyQ Easy Config, you can change the default passwords for login to the MyQ Web Interface and for access to the MyQ Firebird database.

- 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.

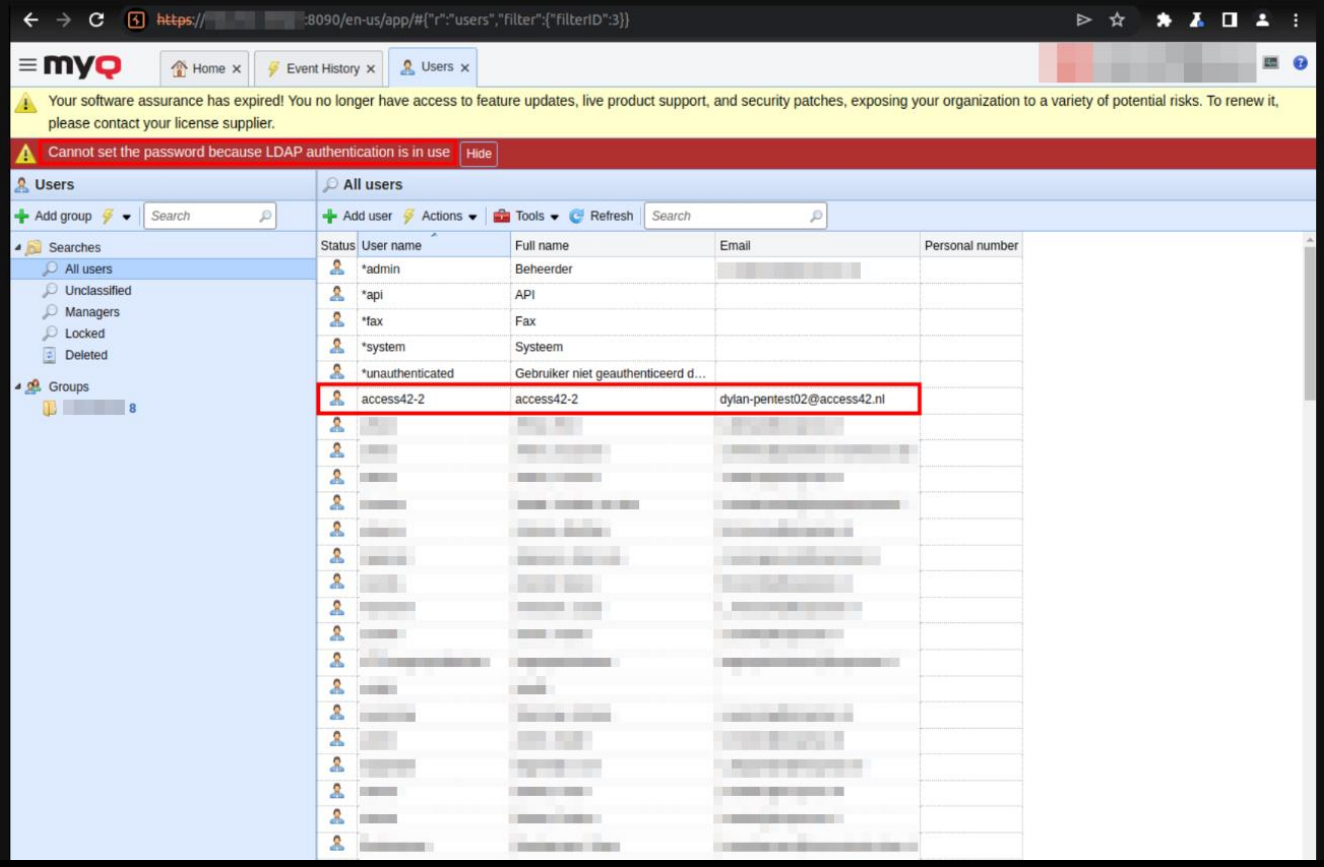
Access to the Dashboard

Interesting features



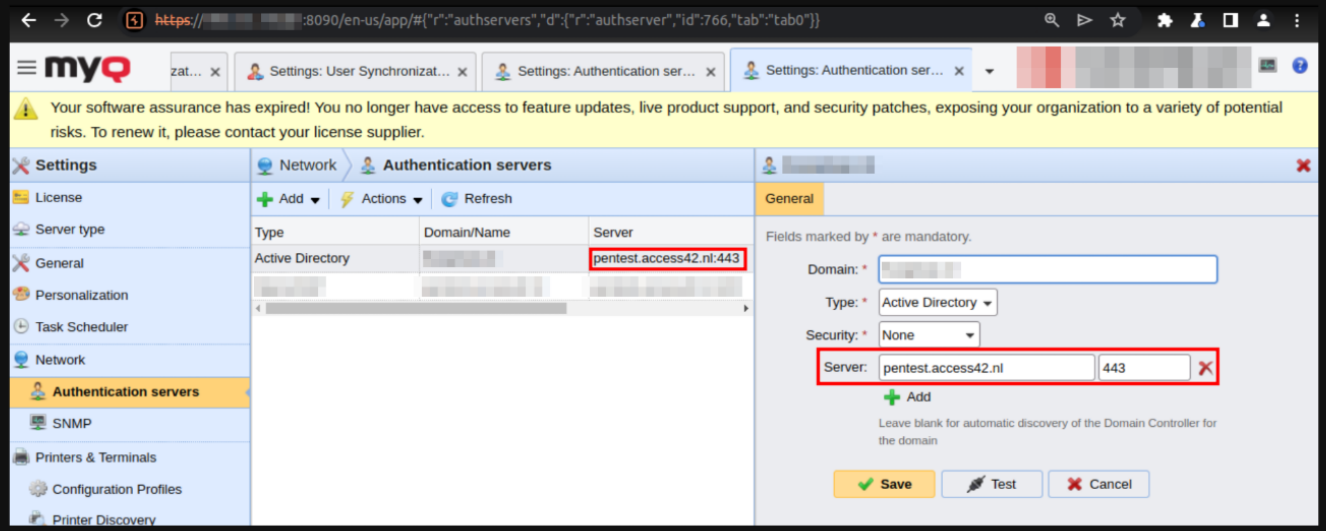
Adding an User

LDAP authentication in use?



Setting up the Authentication Server

This might cause some service disruption...



ACCESS42 Cybersecurity

Password Extraction

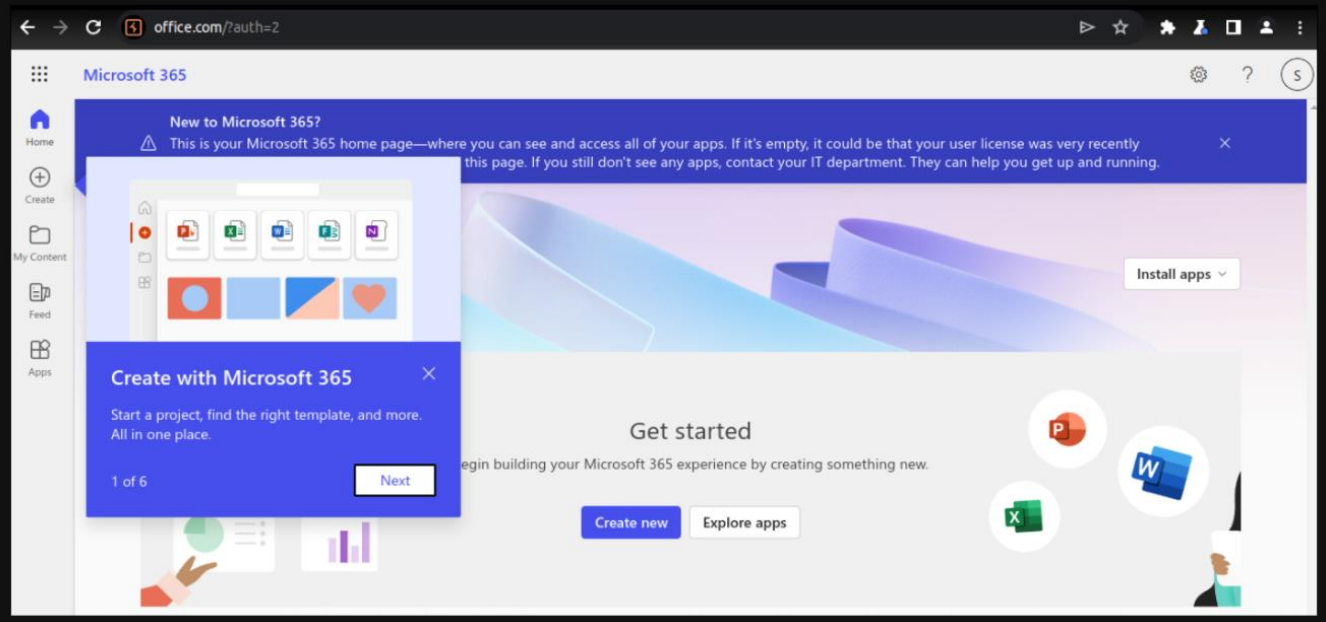
Cleartext password from a service account and encrypted password hashes from domain users

```
# 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
```

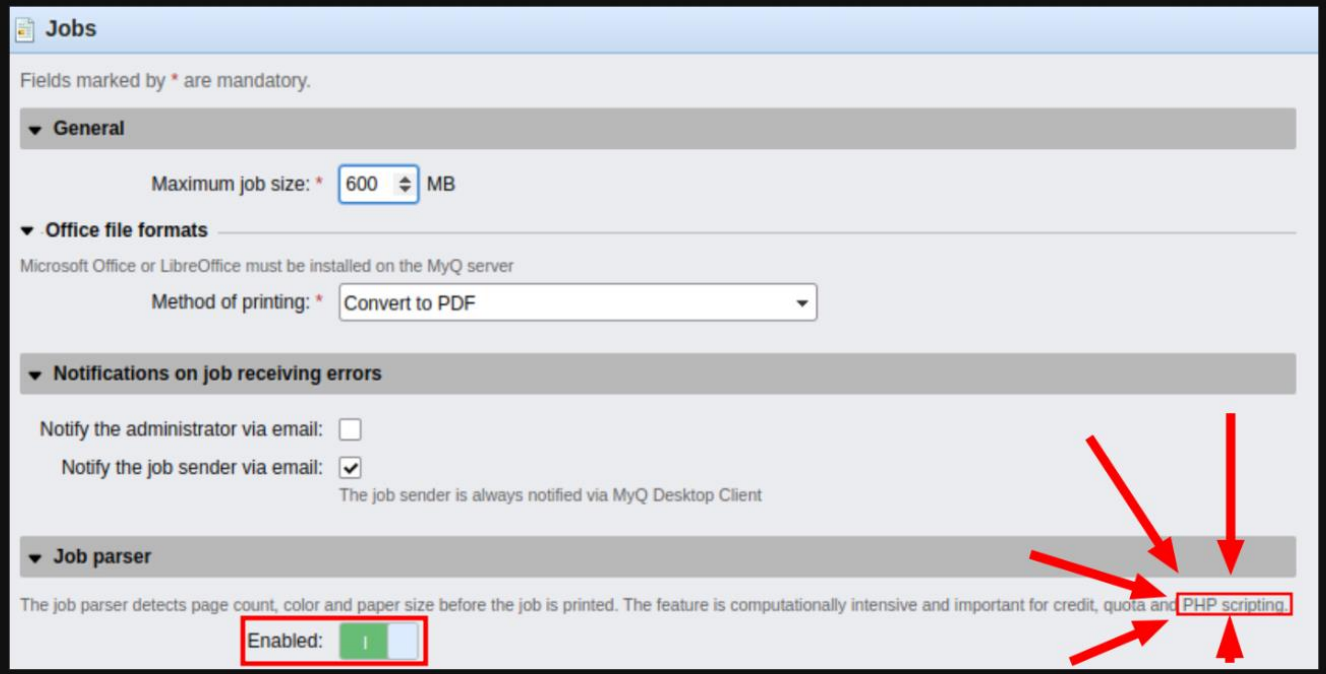
Obtained Access

Working credentials without MFA



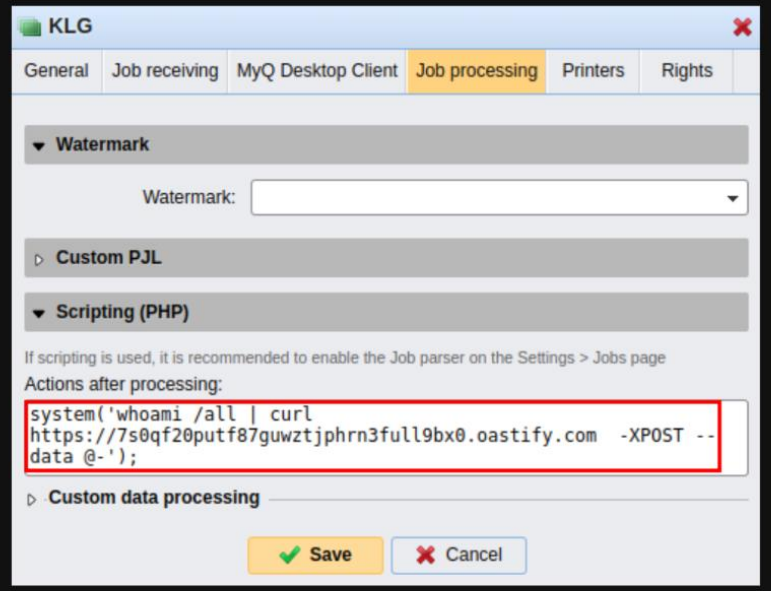
The Job Parser

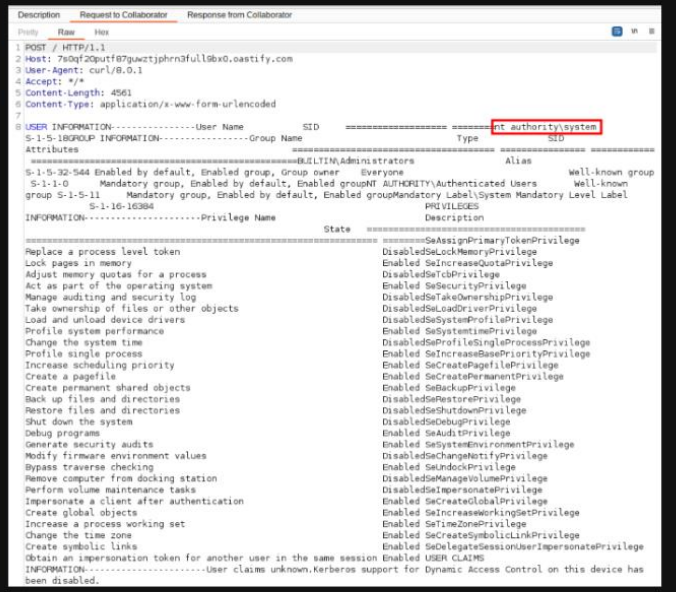
PHP scripting sounds interesting



Obtaining the Output

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





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. Therefor, the attack should be executed in a blind matter.

The 'system' command [1] 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.

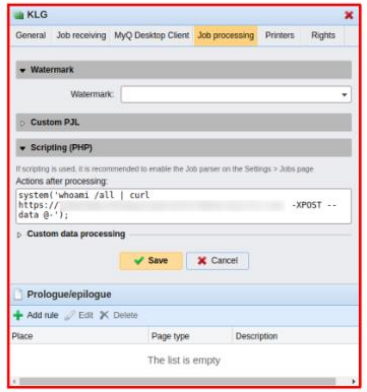


Figure 3: PHP payload

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 MyQ 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 - MyQ 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 MyQ.

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

ACCESS42 Cybersecurity

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

ACCESS42 Cybersecurity

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 Wesselink, Edwin Siebel

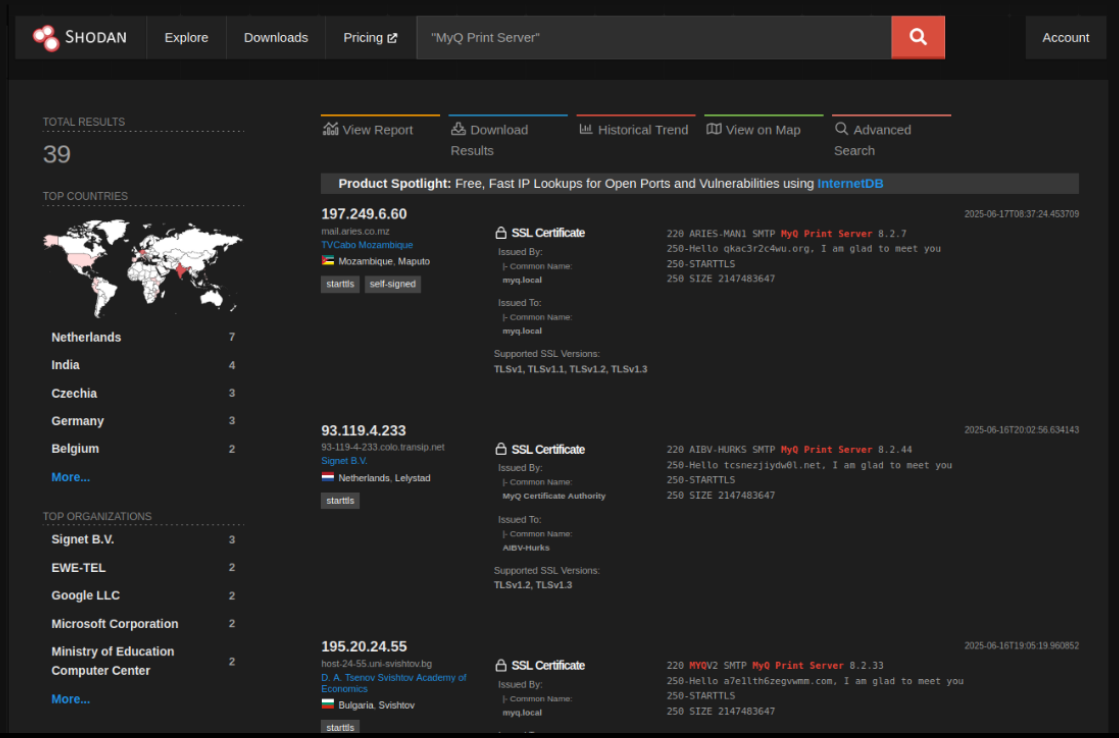
2024-02-15

🌐 Publicly disclosed the vulnerability

ACCESS42 Cybersecurity

The Current Situation

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



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!!!

ACCESS42 Cybersecurity

Thank You!

Dylan Wesselink | dylan@access42.nl

Edwin Siebel | edwin@access42.nl

Let's connect!

Questions?

ACCESS42 Cybersecurity