White paper

Security: best practices for your printing systems

About us

DOXENSE

We've been publishing independent **print and scan management software** for over 20 years.

They enable you to anticipate and **make savings** in energy, money, and time, while reducing your environmental impact.

Simplicity

Security

Environnement

Print, breath !

Summary

1.Introduction

Printing systems are an integral part of a company's technological infrastructure, regardless of its size. However, their security is often overlooked, even though they can be vulnerable to cyberattacks and sensitive data leaks. Cybercriminals are aware of this security gap and increasingly target printers to access confidential corporate data. One notable example is the Print Nightmare, a Microsoft vulnerability that allowed hackers to remotely execute code on a target machine.

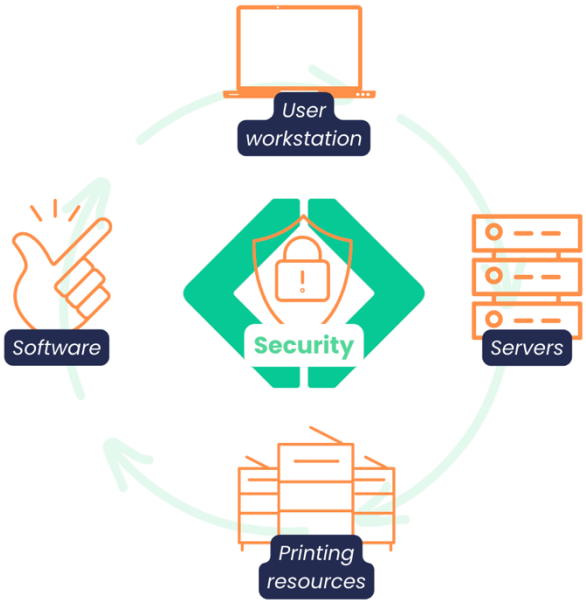
As a result, printer system security has become a major concern for businesses.

The Common Vulnerabilities and Exposures (CVE) is a repository of publicly available information about cybersecurity vulnerabilities and exposures. A search in the repository reveals thousands of vulnerabilities related to printing systems. These vulnerabilities can allow an attacker to view printed documents, use the printing system as an entry point to the company's network, or even take control of your servers.

Here, we present **a set of best practices and security measures** implemented by Doxense consultants.

Doxense's Watchdoc solution offers a comprehensive approach by addressing various aspects:

- Hardware: Security of printers, servers, user workstations, networks, etc.
- Application: Secure printing policies through authentication, pull printing, monitoring, etc.
- Legal: Protection of personal data.



2. User Workstation Security

80% of computer security issues stem from internal human error related to procedural or usage problems, according to the CNIL (French Data Protection Authority).

It is therefore natural to begin this whitepaper with user access security.

a. Authentication

One key aspect of security is user authentication. It is a prerequisite to ensure that each user only has access to their own documents and the assigned printing resources.

The Watchdoc solution addresses this point in two ways:

- At the print server level.
- Directly on the user's workstation.

On the print server, Watchdoc analyzes the spool files and extracts the owner information.

On the user's workstation, the Watchdoc Print Client software (currently available on Windows, Android, and Chrome) directly retrieves the authenticated user account.

It can integrate with the authentication systems of Google and Microsoft Azure AD*. The exchanged token only uses the user's email address and is solely used to verify their identity. Once Watchdoc has verified the identity, it generates its own Refresh Token and uses it to secure communication with the Watchdoc server.

The printed documents are then linked to the accounts registered in the company's directory. Watchdoc allows the use of local directories (such as Active Directory, LDAP), cloud directories* (such as Azure AD, Google), or a guest account database.

b. Connection to the print server

By default, Windows uses the Server Message Block (SMB) protocol for sharing print files. SMB versions 2 and SMB 3 allow for encryption of print files exchanged between user workstations and print servers. **We recommend**

verifying that SMB encryption is enabled and disabling SMB version 1 (which is no longer present on workstations since Windows 10 and servers since Windows Server 2019).

The Watchdoc Print Client* software eliminates these issues by securely handling the transfer of print documents. **Communication is encrypted end-to-end** using the HTTPS protocol and supports TLS 1.2.

Authentication between the client and the Watchdoc server utilizes the OAuth protocol. This ensures that only an access/refresh token is stored, and no sensitive data (such as user login or password) is retained.

c. Secure driver deployment

Since Windows 10, Microsoft has enhanced the security of driver installations by allowing only drivers certified by Microsoft. Publishers are required to adhere to the Microsoft Windows Hardware Developer Program and prove their identity by providing an Extended Validation (EV) code signing certificate. **This certificate, obtained through a rigorous verification process, ensures that end-users can trust that the publisher's identity has been verified.**

Watchdoc Print Client* enhances security by ensuring that the deployed driver is the one loaded by the administrator. This means that it is impossible for a third party to compromise a driver and have it deployed by Watchdoc.

3. Server security

After addressing user workstations, it is undoubtedly essential to consider server security.

a. Print server

Security best practices must be implemented on print servers. Here is a list of key points:

- The hardware should be monitored to anticipate any failures or disk storage saturation.
- The operating system should be kept up to date, at a minimum for security vulnerabilities, but ideally on the latest version of the system to disable outdated protocols, such as SMB v1 mentioned above.
- The server should be protected by an antivirus software, and it should be regularly updated.

- Access to the server should be restricted to administrators only. Network shares should be restricted as much as possible.
- The print server should not be accessible from a public network. Its access should be restricted to an internal network or a DMZ (Demilitarized Zone).
- The print server and the database should be backed up and included in the Disaster Recovery Plan (DRP) for business continuity in the event of a disaster).

b. Print queues

Modifying the configuration of print queues is reserved for system administrators.

We recommend **avoiding the use of the LPR** (Line Printer Remote) protocol because it does not verify the user's identity and is not sufficiently secure. Its usage should be restricted to legacy applications (such as AS400, Mainframes, ERP) or ideally **blocked by closing its port 515.**

Servers store print documents on their disks in files called "spool" files. By default, these files are not encrypted, which means that anyone with access to the server can access the content of these files. **The Watchdoc solution addresses this issue by encrypting the spool files**.

Lastly, **Watchdoc allows for the configuration of print queue visibility and restriction of their rights**, such as access to colour printing, scanning, and more.

c. Drivers

Print drivers are installed on both servers and user workstations. **It is crucial to ensure that no malware is inserted into a driver to prevent its spread within the company's network**.

To address this, since Windows 10, Microsoft allows the installation of drivers that have been certified through the Windows Hardware Compatibility Program.

With Watchdoc Print Client, we enhance this security by ensuring that the deployed driver is indeed the one loaded by the system administrator.

Watchdoc's **Driver Store* is a Trusted Store** that utilizes X.509 certificates stored in the PKCS#7 format. The certificate used to sign the driver must be approved by both the print servers and user workstations.

We recommend having the network administrator sign the driver on a different server than the Watchdoc server. This ensures that the private key is not accessible to an attacker who may have compromised the Watchdoc server. The Watchdoc server should only retain the public certificate so that clients can verify the driver.

4. Securing printing resources

After addressing users and servers, we now turn our attention to the devices involved in document printing. This includes both the copiers themselves and the network infrastructure, documents, and authentication.

a. Multifunction copiers and printers

Here are some best practices regarding multifunction copiers:

- Update the firmware regularly.
- Do not leave default manufacturer passwords in place.
- Block USB ports and disable unused interfaces such as Bluetooth, Wi-Fi Direct, and NFC.

In general, **it is advisable to adopt a Zero Trust approach** by closing all ports/protocols and only keeping those that are actively used.

We recommend not using the LPR, RAW, and IPP protocols as they are not encrypted, which means that the content of the documents is transmitted in clear text over the network. It is advisable to **prioritize multifunction copier models that support the IPPS protocol** while taking care to disable SSL 1.0/2.0/3.0, TLS 1.0, and TLS 1.1 protocols, leaving only TLS 1.2. Implementing this encrypted protocol requires deploying a certificate on the copier using manufacturer tools. **We recommend using a certificate generated by an internal Certificate Authority (CA) within the company**.

b. Network

Just like print servers, printers are not intended to be accessible from a public network. Their access should be restricted to an internal network or a DMZ. **The ideal configuration is to place printers in a dedicated subnet that is only accessible by print servers**.

Disable all unencrypted access methods, such as HTTP commonly used for administration consoles, FTP used for document transfer, LPR, RAW, IPP, etc.

c. Documents

A good practice is not to keep a copy of printed/scanned documents on the machine's hard drive. Therefore, it is **recommended to enable regular disk purging**.

We also recommend **prioritizing models that allow for disk encryption**.

d. Authentication

By default, multifunction copiers are secured with a single administrator account. All users use the same anonymous access. In addition to changing the default password for the administrator account, it is important that each user can have their own personal access in order to ensure they cannot see documents printed/scanned by other individuals.

To address this requirement, the Watchdoc solution offers the deployment of the **Watchdoc Embedded Solution** (WES) module on multifunction copiers. **This module secures access to the copier** by requiring users to authenticate themselves with a code or badge in order to access their personal space. They will only have access to their own documents, ensuring privacy and security.

5.Software security

Last but not least, in our white paper, software security is essential to protect against attacks.

a. Printing solution

The printing solution, like any other software solution, can be compromised by a third party. It should not run with a local root/administrator account to ensure that access to this account is not provided. It should particularly not run with a domain administrator account. We recommend using a service account that has the necessary rights, such as the ability to interact with the spooler.

The code of the solution **must be signed with a dedicated certificate**. This ensures that the software provided by the vendor has not been tampered with or modified by a third party. The software in the **Watchdoc solution is signed**

with a DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1 certificate.

It is the responsibility of the vendor to implement a secure development policy, ensure protection against attacks (including the OWASP Top 10) on the administration interface, and secure access to its API.

The administration interface should only be accessible remotely if it is secured through access with enterprise directory accounts. **The Watchdoc solution supports Active Directory, Azure AD*, and LDAP directories**.

For maintenance purposes, the solution may allow the use of an admin password, provided that it is encrypted and that this access is only possible from the server itself (localhost). Watchdoc is compliant with these requirements.

b. GDPR

The printing solution must comply with the General Data Protection Regulation (GDPR) adopted in 2016 by the European Parliament. In the case of an on-premise solution, the software should enable every user to exercise their right to be forgotten, also known as the "right to erasure." **The Watchdoc solution allows for anonymization of personal data for users**. This method allows for the retention of statistics while respecting the principles of the GDPR.

c. Solution maintenance

The software solution should be regularly updated to benefit from security patches. It is advisable to choose a vendor that has implemented a secure development policy and regularly undergoes audits of its solution.

d. Access rights

A printing solution is a product that handles sensitive or sometimes confidential information. It is therefore important to be able to assign management rights specific to each profile/user.

The **Watchdoc solution allows for fine-grained access control**, for example, on user management, print queue administration, quota management, access to statistics, or document preview.

e. Printing policy

Not all printing devices should be accessible to all users within a company. The print solution should restrict access to specific users or user groups.

To control printing costs, the solution should also allow the implementation of rules. For example, certain devices may not accept colour printing except for the Marketing department, or large print jobs should be redirected to the appropriate equipment.

To finely control printing costs, **we recommend solutions that allow for quota management**. A quota is a credit of units dedicated to printing and assigned to a user or group of users. In case of internal cost allocation, these quotas can be monetized. This is referred to as a virtual wallet or virtual currency system.

f. Document release

The printing solution must ensure that each printed document is retrieved by its owner. Without a printing solution, a printed document goes straight out and waits for the owner to come and collect it. Too many documents are left on printers, end up in the bin or are inadvertently retrieved by someone else. **And this raises the problem of document confidentiality**.

A secure release solution means that users can only release their documents when they are physically in front of the printing device.

This makes it possible to manage another problem: in the event of a breakdown (paper jam, lack of toner), the documents remain in the printer. As soon as the breakdown is resolved, without a secure release solution, all the documents are removed at the same time. They generally end up in the bin.

The **Watchdoc Embedded Solution (WES) secure release module goes further by encouraging users to reduce their printing costs**, by switching from colour to black and white, or to duplex printing, for example. Document previewing also enables unnecessary pages to be removed before they are printed.

g. Confidentiality

As we have seen, a secure release solution ensures the confidentiality of documents when they are printed.

On user workstations, with a Windows shared print queue, all users can see the name of all printed documents.

The Watchdoc solution solves this problem in two ways:

- On the server side, Watchdoc anonymises document names. Users can still see the full list of pending documents while respecting their confidentiality.
- With Watchdoc Print Client*, we no longer use Windows shared queues; **users simply have access to their documents**.

h. Deleting pending documents

With a secure release solution, a key cost-saving feature is **the automatic purging of documents that are not released**. For example, in Watchdoc, by default, any document not printed after 48 hours is automatically deleted.

i. Tracking

By generating savings, particularly in terms of natural resources, **a printing solution is part of a company's CSR policy**. The success of such a policy depends on employee involvement. The printing solution must provide individualised indicators so that employees can become aware of the environmental cost of their printing.

The **Watchdoc solution makes it possible to communicate individually to employees about their printing costs but also, and above all, about the savings made by their good practices** (switching from colour to black and white, simplex to duplex, deleting unnecessary pages, documents not printed).

To find out more about our solutions, got to:
www.doxense.com

* Available from Watchdoc V6

BIBLIOGRAPHY :

https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-security

https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

https://learn.microsoft.com/en-us/windows-hardware/drivers/install/digital-signatures

https://learn.microsoft.com/en-us/windows-hardware/drivers/install/kernel-mode-code-signing-policy--windows-vista-and-later-

https://www.digicert.com/kb/digicert-root-certificates.htm

https://owasp.org/www-project-top-ten/

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article17

https://doc.doxense.fr/fr/Watchdoc/Content/C_Configurer/FR/ConfigDroits/ConfigDroits_Detail.htm

https://doc.doxense.fr/fr/Watchdoc/Content/H_HowTo/FR/WD52_Anonymisation_Procedure.htm

https://doc.doxense.fr/fr/Watchdoc/Content/H_HowTo/FR/WD5_Regles_Presentation.htm

https://doc.doxense.fr/fr/Watchdoc/Content/C_Configurer/FR/ConfigTarifs/ConfigTarifs_Principe.htm