

WHITEPAPER

UNDERSTANDING MULTIFUNCTION PRINTER (MFP) SECURITY

WITHIN THE ENTERPRISE BUSINESS ENVIRONMENT

Deral Heiland - Principal Security Researcher IoT
Sam Moses - Security Consultant Penetration Testing



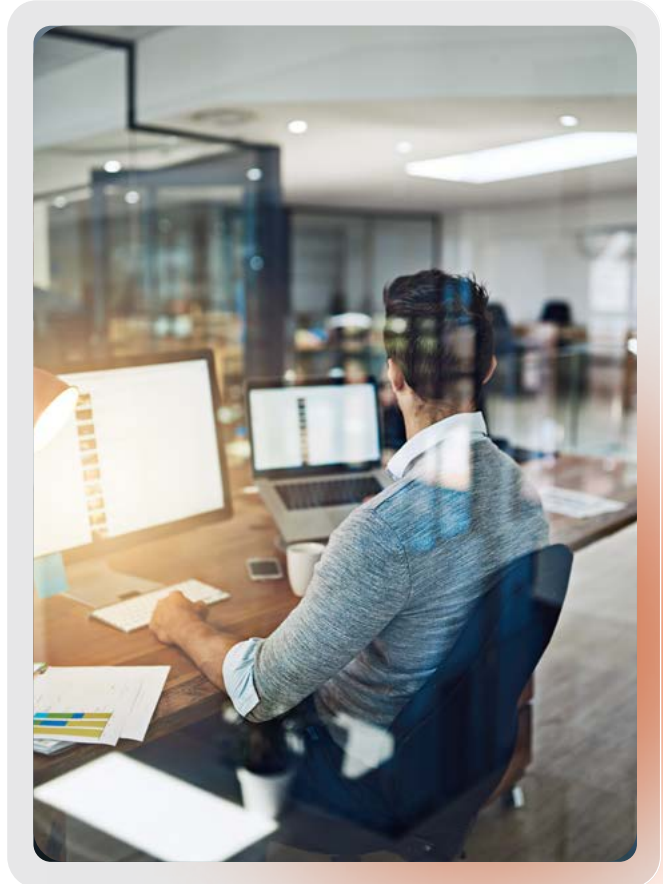
RAPID7

Introduction

The goal of a completely paperless workspace has been years in the making. Advancements in multifunction printers (MFP) devices have brought us closer to that goal. The features and capabilities of modern MFP devices have made it possible to avoid just printing everything. These devices have allowed us to deeply integrate paperless features into our business environments, allowing us to scan and send and receive documents via file shares, emails, faxing, and other internet services between employees and business partners without ever requiring the document to be printed.

With those amazing capabilities also comes greater responsibilities and risk. Since these devices can and are integrated throughout most business environments, the security implications are far reaching. In this paper we plan to discuss those security implications from historical to current issues, vulnerabilities, and risks. It will look into how those concerns can negatively impact our security posture if not addressed and how best to address these security issues.

With that said, the overall purpose of this paper is meant to provide value to a wide range of readers, from technical folks dealing directly with MFP devices in deployment and support roles to those involved in managing organizational security or governance. The goal here is to give each audience the insights they need to better understand and mitigate the risks tied to these MFP technologies currently deployed in every enterprise organization.



MFP technology and common security issues

In general, [MFP devices](#) first got their start when manufacturers sought to reduce machine footprints within office space areas by combining copy machines and printers into a single device. Over time more features have been added including faxing, email, file sharing services, and document storage capabilities. As MFP capabilities grow so does the security risk and potential impact to businesses.

Security issues and vulnerabilities in MFP devices have a long and tortured history, exacerbated by the fact that many organizations rarely consider security of these devices when deploying them. This can include a lack of patching the devices when vendors release them and not changing the default passwords.

But first, a personal anecdote from Deral Heiland around his interaction with MFP devices. Back in 2008 he landed his first job as a pentester and as he learned the craft of conducting security testing, and writing thorough reports, he regularly encountered different MFPs. He asked his coworkers if they had any good hacks or attacks against MFP devices. The answer he got back surprised him. In general, it was a simple idea: “other than maybe stealing documents off the printers, printers don’t have any real good usable data that can help us during pentesting, so we just ignore them for the most part.”



So, with that information, he decided to explore MFP devices deeper and see if that statement was true. Since most organizations never bothered to change the MFP’s default password, it was simple to login to the device’s web management interfaces and explore. It did not take long to realize that printers had become way more advanced than initially thought.

MFPs have added many new capabilities which allowed deeper integration into our business environments. Not only can we print and scan with these devices, we can redirect print jobs to email and to various file systems using File Transfer Protocol (FTP), Server Message Block (SMB), along with integration into Windows active directory authentication services using Lightweight Directory Access Protocol (LDAP) and Kerberos to authenticate and validate users on the MFP. I quickly concluded that MFPs were potentially a wealth of information any malicious actor could leverage to further compromise an organization.

Once that was figured out, the next step was to determine how a malicious actor could get access to the businesses’ MFP integration information, such as SMB, EMAIL, LDAP passwords, etc.

Early on, you could often just look at the web source code of the configuration pages and find the passwords stored there in clear text for many of the MFP devices I encountered. But soon after we started disclosing these security issues, vendors corrected those problems. The next broad sweeping MFP security issue we identified allowed a malicious actor to make simple changes to MFP configurations to trick the device into forwarding Windows Active Directory (A/D) authentication credentials back to the malicious actor over the network. This issue was coined in 2011 as a [pass-back attack](#). The pass-back attack vulnerability is still currently very much alive and exploitable in many [current models](#) of MFP devices.

Beyond the pass-back attack, several other common security issue categories have been observed over the last decade or so. A few are outlined below.



Printer language attacks (PS, PJP, PCL)

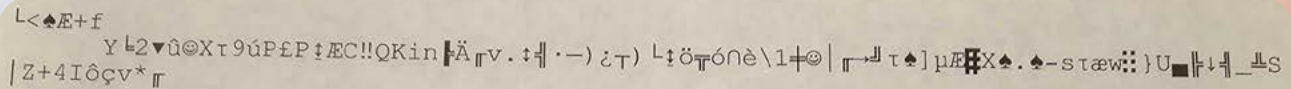
Printer language attacks — those leveraging Printer Job Language (PJP), PostScript (PS), or Printer Command Language (PCL) — can pose a risk to enterprise operations because these languages allow direct, low-level control over how printers process jobs. An attacker leveraging these different printer languages would have the ability to alter the MFP device's functionality to gain access to data storage, disrupt operation or in some cases take full control of the MFP device to execute their code on the devices.

A fascinating example of this type of vulnerability is addressed in the research work conducted by Andrei Costin. During his research work Andrei discovered that PostScript language could be used to place an MFP device's PostScript interpreter into executive mode^[1] allowing for various forms of code execution which could lead to an MFP device being fully compromised.

The open source printer security testing tool, [Printer Exploitation Toolkit \(PRET\)](#), leverages these various printer languages to gain access to print jobs, file systems, memory, and potentially negatively impact the functionality of the MFP devices.

[1] Hack in the Box Security Conference. June 20, 2012. #HITB2012AMS D2T1 - Andrei Costin - PostScript - Danger Ahead - Hacking MFPs, PCs and Beyond [Video]. YouTube. <https://www.youtube.com/watch?v=053TrAcqVOU>

An attacker can also leverage these printer languages to disrupt normal workflow. When exploited, attackers can send malicious or malformed commands forcing printers into endless print loops, continuously printing junk data, as shown below. Also printing arbitrary or offensive content, or rendering devices unresponsive through Denial of Service (DoS), are possible.



L<♠Æ+f
Y 2▼û©Xτ9úP£P!ÆC!!QKIn Ä v. ‡|| ·-) ¿T) L‡öTóNè\1‡⊕| ||τ♠]µÆ#X♠.♠-sτæw::}U■||↓||_♠S
|Z+4Iôçv*||

FIGURE 1

An example of **junk data** printed by an attacker

These types of attacks not only disrupt normal workflows, but deplete toner and paper supplies. Left unchecked, printer language abuse, whether an accident, error, or from malicious intent, can halt document workflows across departments and undermine productivity.

Firmware alteration attacks

Another attack path discovered on MFP devices are attacks targeting the MFP firmware and its update processes. With these attacks, malicious actors have been able to alter the firmware and deploy it over the network to a targeted MFP. This allows a malicious actor to take full control of an MFP and, in cases where the printing services were exposed to the internet, allow a malicious actor to send a print job to trigger this exploit over the internet and have the printer phone home allow the attackers to pivot through the MFP from the internet to the internal network. An example of one such attack method is documented in the blog [Advanced Persistent Printer](#).

Information leakage attacks

Another common issue with MFPs is information leakage vulnerabilities. Information leakage happens when a person or system within an organization exposes internal information. Due to lack of security controls, weak configurations, outdated systems or software vulnerabilities, printers can end up exposing internal information to attackers to allow them to gain details needed to obtain a foothold or perform lateral movements. Information leakage with printers could include usernames, domain service information, stored files, serial numbers, and in extreme cases, sometimes passwords.

A great example of this style of vulnerability, [CVE-2024-51977](#), was recently identified by Rapid7 Security Researcher Stephen Fewer. Stephen also released a technical analysis in which he described how exploiting this data leakage allowed for additional vulnerability exploits against the targeted Brother printer. A detailed writeup of the Brother MFP vulnerabilities is available [here](#).

Pilfering data from decommissioned printers

A commonly overlooked security issue involving the improper decommissioning of MFP devices could potentially impact your organization. This issue arises when an organization does not have detailed processes and procedures for decommissioning embedded technology such as MFPs. At the end of life of an MFP device, organizations often just roll it to the loading dock and it is hauled away. The device is often just resold with the original owner unaware that they just sent potentially critical internal information, such as stored documents and account information that are easy to extract from the device, out the door.

For example, we purchased a few used current model MFP devices for a research project and discovered one of the devices was still configured with the previous organization's information. This included employee email addresses and user account information including Windows Active Directory passwords. During another previous MFP project conducted several years ago, We visited a large warehouse containing thousands of used MFPs. We were there to purchase a device for developing some Metasploit modules. During that visit we tested the device we planned on purchasing and found it contained the previous business owner's data. The manager running the warehouse was shocked because he had assumed the data had been purged prior to shipping to him. Out of curiosity he had us test a half dozen more devices, and we found three of those MFPs still contained data (AD passwords), for example.

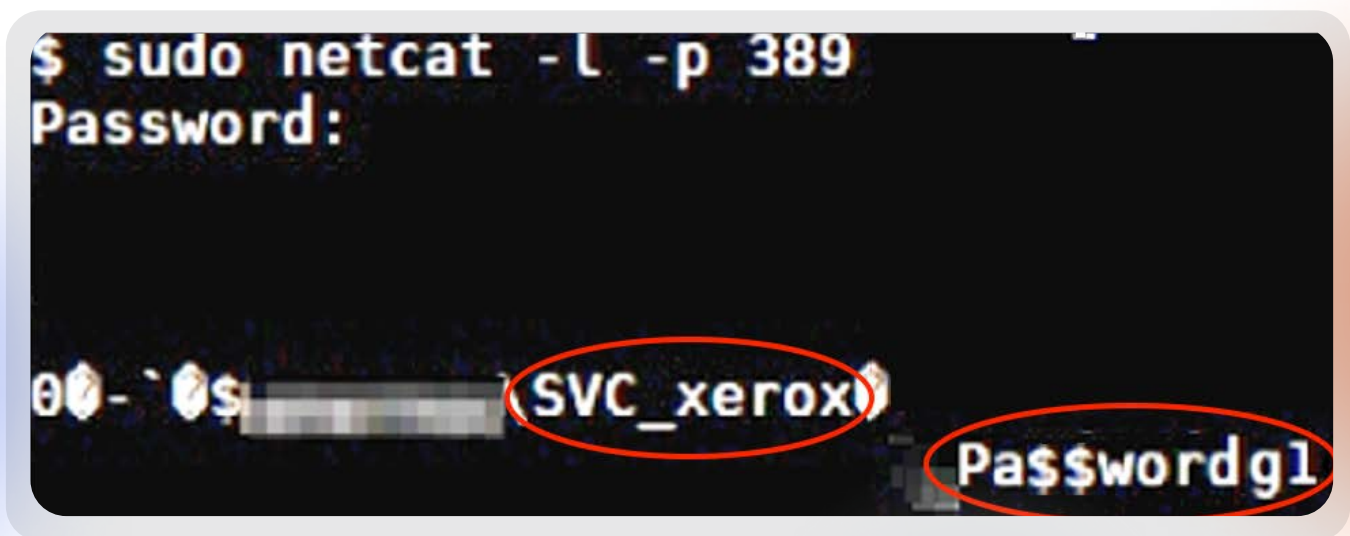


FIGURE 2

Examples of data still existing on
decommissioned and resold MFPs

During the following conversation I asked him where all of these MFPs were being shipped to? He informed me that over 90% of them were going to end up shipped to Asia — with all data and passwords still intact. Let that sink in. You may think user passwords get changed on a regular basis, which is true, but generally we also typically find AD service accounts being used on MFP devices. The example shown above is SVC_xerox. Rarely are those passwords ever changed in most organizations.

Security impact

The potential impact to an organization from these attacks can vary but, at a minimum, a malicious actor can leverage these attacks to do the following.

- **Extract critical internal data**
 - Personally Identifiable Information
 - Password and account data
 - Corporate confidential business data
- **Conduct credential compromise**
 - Capture stored service accounts (LDAP, SMB, FTP, email relay credentials)
 - Intercept usernames and passwords sent via unencrypted protocols
- **Breach an organization's perimeter security**
 - Exploit internet-exposed printers to bypass firewalls
 - Turn a "trusted" device into a stealthy entry point
- **Network intrusion and lateral movement**
 - Use the printer as a pivot point into internal systems
 - Establish persistence that often goes undetected due to weak monitoring
- **Operational and business impact**
 - Disrupt daily operations (printing, scanning, etc.)
 - Create regulatory non-compliance
 - Result in financial loss from incident response, downtime, and potential fines
 - Cause reputation damage and loss of partner trust

MFP Exposure

In this section we focus on exposure and risk by examining a number of MFP brands and their exposure to the internet, vulnerabilities, and examination of historical penetration testing data.

Internet exposed MFPs

Generally, MFP devices should never be exposed to the internet. Such exposure increases the probability of compromise, which could lead to a breach of the organization. During this research I leverage Shodan to identify devices exposed to the internet. To narrow the scope down I focused only on higher-cost MFP devices, greater than \$500, which are more likely to be used within small-to-large organizations. During this research we identified more than 5500 MFP devices on the internet. In the following diagram we have broken the list up to eight of the most common MFP brands on the market and the number of devices identified for each brand on the internet via Shodan.

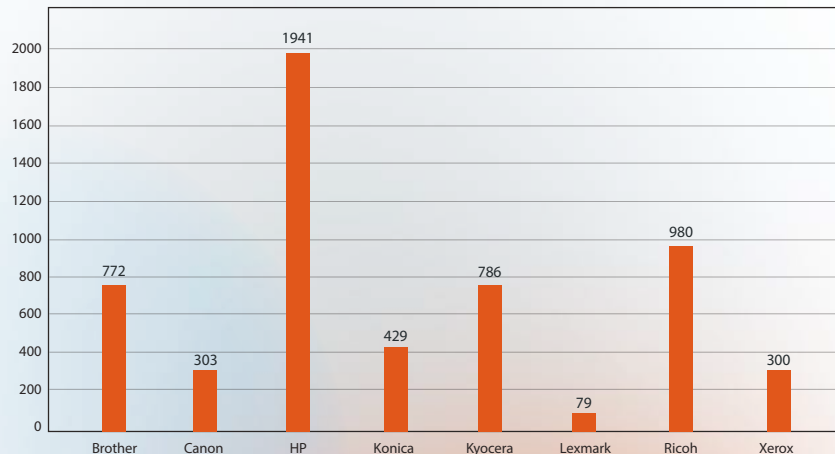


FIGURE 3

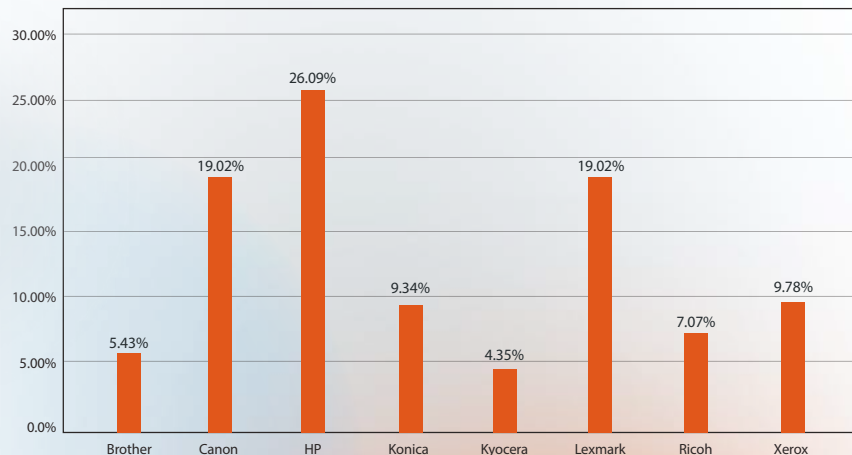
The **eight most common** MFP brands and the number of devices of each

Common vulnerabilities and exposures

Next we focused on the [Common Vulnerabilities and Exposures](#) (CVE) database to identify vulnerabilities published over the last four years (01/01/2021 - 09/15/2025) impacting the eight MFP brands identified above on Shodan. During the examination of the CVE database we found a total of 164 CVEs. A percentage breakdown of these CVEs and the brands impacted by them is shown here:

FIGURE 4

The percentage of the **164 identified CVEs** which impacted each brand



Further examination of the 164 CVEs found that 51 of the CVEs had no Common Vulnerability Scoring System (CVSS) scores, leaving only 113 CVEs with assigned CVSS scores. Several of the CVEs also had multiple impacted devices and, in some of those cases, the different devices had different CVSS scores; giving us a total of 121 CVSS scores from the 113 CVEs. Below is a breakdown of the severity ranges of CVEs based on the identified CVSS scoring for the MFPs.

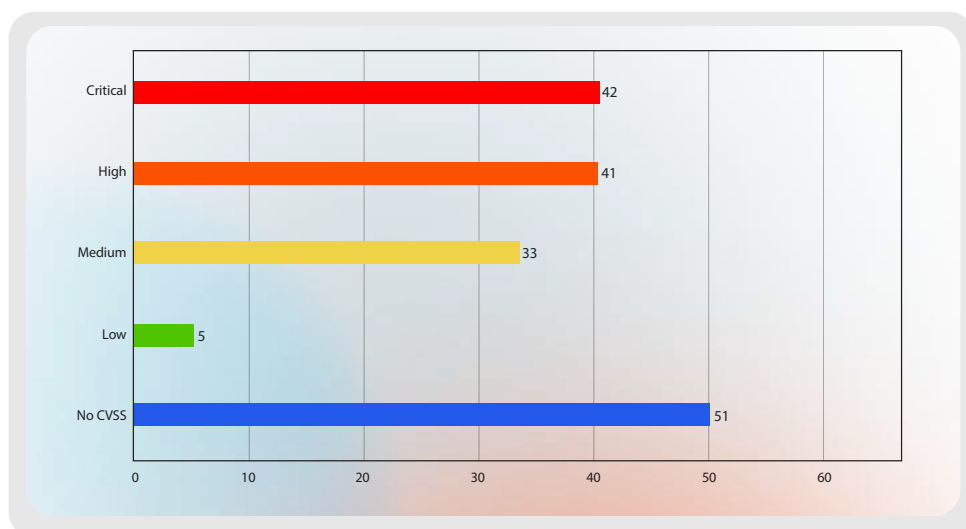


FIGURE 5
Severity ranges of CVEs based on the **identified CVSS scoring** for the MFPs

Over 37% of the CVSS scores identified fall into the Critical categories with a Critical CVSS score of 9 or higher. We then examined those CVEs with Critical CVSS scores to identify the Common Weakness Enumeration (CWE) identification for each. The following table identifies these CWE lists from most common to least common.

Common Weakness Enumeration (CWE)	Count
CWE-787 - Out-of-bounds Write	15
CWE-20 - Improper Input Validation	5
CWE-121 - Stack-based Buffer Overflow	5
CWE-120 - Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	3
CWE-122 - Heap-based Buffer Overflow	2
CWE-22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1
CWE-119 - Improper Restriction of Operations within the Bounds of a Memory Buffer	1
CWE-125 - Out-of-bounds Read	1
CWE-129 - Improper Validation of Array Index	1
CWE-190 - Integer Overflow or Wraparound	1
CWE-362 - Race Condition	1
CWE-400 - Uncontrolled Resource Consumption	1
CWE-522 - Insufficiently Protected Credentials	1
CWE-807 - Reliance on Untrusted Inputs in a Security Decision	1
CWE-843 - Access of Resource Using Incompatible Type ('Type Confusion')	1

Many of the above CWEs open up the MFP devices to some form of full remote compromise and remote code execution. Having devices on the corporate network vulnerable to these style of attacks should be avoided. To accomplish this goal it is always recommended that all MFP devices be included in your organization's internal patch management program and ensure all MFP devices are regularly patched with the latest security patches supplied by the vendor. Also, on a positive note, during this review of the 42 critical vulnerabilities we also researched their patching status and found only one of the vulnerabilities did not have a patch released by the vendor to fix it. In that case, CVE-2024-51978, it was recommended by the vendor to change the default password to mitigate the risk. This shows that vendors are overall diligent in releasing security patches for their products when critical vulnerabilities are found and also highlights the value in regularly applying vendor security to your MFP devices.

Pentest exposure of MFPs

As part of this study, we also examined data obtained from security assessment pentests performed by both [Rapid7](#) and [Raxis](#) between 2020 and 2025. Data related to MFP security issues was obtained from a total of 136 assessments. These assessments showed 121 of the organizations tested had MFP devices on their network where default credentials were still enabled, allowing admin level access to the MFP devices during 97 of those engagements. Also, pentesters were able to successfully leverage the common MFP pass-back attack to enumerate credentials, allowing them to gain some level of access into the organization's Active Directory Windows environment. During these assessments, the pentesters were also able to enumerate further data from the MFP devices including documents and user data. Typically this user data included email addresses and usernames which they were able to leverage during the assessment using other attack and penetration methods.

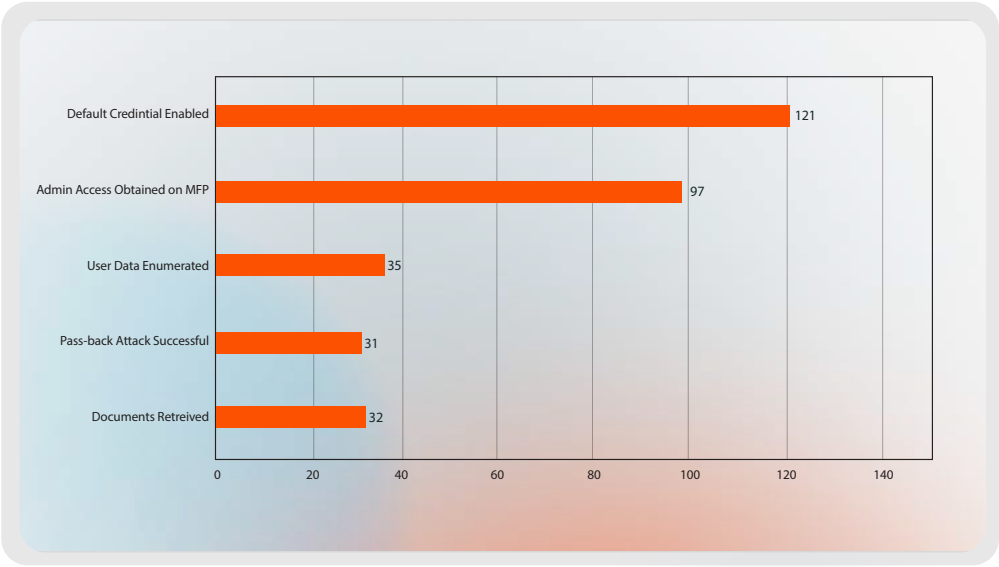


FIGURE 6
The number and type of **successful penetration** test yield

This data highlights the criticality of not changing the MFP's default password and potential impact of a pass-back attack, especially if the account stolen from the MFP devices happened to allow elevated level access into Windows Active Directly environment.

Mitigation and managing risk

In our opinion the most common MFP vulnerability has been the pass-back attack. This issue has continually plagued MFP devices for over a decade and, until recently, little effort has been made to resolve this issue in spite of it being reported many times to the MFP vendors. Some of the vendors have recently started working on resolving and/or mitigating this issue by either fixing the core problem or just forcing the user to change the default password during MFP setup. The core problem being that a logged-in user can change the IP address to an authenticated service such as SMB, LDAP, SMTP, without being forced to re-enter the services password, making it simple to redirect the service authentication, capture the password in clear text, and gain access to other critical services outside of the MFP device.

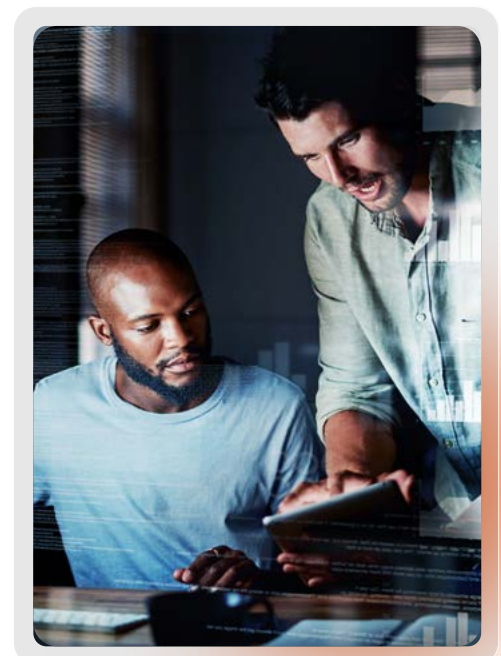
But other vendors, as mentioned above, have only worked on a mitigation of the issue by forcing password changes during the device setup so the devices no longer have a default password enabled. Both of these need to be done to remove the security issues.

So how can organizations protect themselves from MFP security issues, such as these, moving forward? Basic security hygiene plays a critical role in protecting organizations from MFP security issues. And that starts with the device's passwords. Failure to change default passwords has been a major concern since these machines have been introduced. With that said, most credentials and data extraction attacks on MFPs can be thwarted by simply setting a complex password for the device's administrator account. Second, organizations should focus on patch management to ensure that when a vulnerability is discovered and fixed by the vendors, that the MFP environment is patched so fewer fall victim to being exploited.

On a bigger scale, which goes beyond just MFPs, organizations need to develop a comprehensive cradle-to-grave program that defines policy and process covering all new embedded technologies entering the workplace. These policies and processes should include acquisition, deployment, support, and de-acquisition.

During the acquisition of an MFP, organizations should consider more than just the cost of the machine itself. Other key areas include product security, how the vendor handles vulnerabilities when they are reported, and how long it typically takes for vendors to patch a vulnerability when it is reported. Also, product features and functions should be considered. If you want to just print and nothing else, why buy a printer that integrates into email, Windows authentication, or other advanced features such as document storage? These advanced features add more risk to the equation and when not being leveraged, often go unconfigured. Also, where possible, organizations should own the MFP. But, if leasing the MFP, organizations should know what language needs to be considered in the contract to protect data and networks from potential security issues arising from poorly managed MFPs under contract.

When considering the purchase and deployment of new MFP devices within your organization there are a number of things that should be addressed. Here is a short checklist of those items to help to improve your overall security posture.



1. Do the legwork upfront when buying MFPs and consider the following:

- a. Does the vendor supply security patches even if you don't pay them for a service contract?
- b. Does the vendor have a regular patch management cycle?
- c. What is the vendor's track record for patching disclosed vulnerabilities?
- d. Do you buy the printers or just lease them? If leasing, consider any security requirement in the legal contracts including disposal at the end of life.
- e. If you do not need the bells and whistles that allow integration into Windows Active Direct, email, or other services or color consider purchasing lower-cost printers with fewer features.
- f. Consider MFP devices that have enterprise management solutions so they can be globally managed and monitor your MFP environment.

2. Change the default password to something complex that does not match other non-printer devices within your current infrastructure.

3. Place the device into a patch management cycle and track vendor patches so they can be deployed when released.

4. When integrating your MFP into your business environment, such as SMB scan to file, Scan to Email, LDAP authentication, do not use accounts with elevated rights and ensure that the accounts are restricted to only what is needed. For instance, do not set up LDAP services on the printer to use a Domain Admin account.

5. Properly network segment MFP devices based on their business purpose. For example: HR, Payroll, Executive MFPs should not be accessible from the general employee network segments.

6. Make sure you have a plan for decommissioning the device when you purchase it and don't wait until the end-of-life to consider those critical questions.

Auditing MFP security

One big question we are often challenged with is how to identify MFP devices that may be a security risk because of poor setup and configuration issues. For example, it is not uncommon to encounter organizations that ask during security assessments to not bother to look at their MFP devices because they know they are not secure. We often struggle with these concepts. If they know they are not secure, why would they not try to just fix the issues and remove this concern off the table? Although, if we think this through we can probably identify the possible cause of this and it most likely falls within the following categories:

- **They do not truly understand the potential risk to their organization.**
- **They think their MFP devices are not actually configured for any real business enablement features. So they do not see the potential risk.**
- **The organization does not have the manpower and resources to address the issues.**

Either way, it is critical that organizations understand the potential risk of vulnerable and exploitable MFP devices. Even if a malicious actor may not be able to steal critical data directly from your devices, because they are not configured for enterprise integration, they can still often be used to hide their nefarious activities on your network. Such as: store attack tools, pivot their attacks through your network, and/or exfiltrate data from your network.

With this said, we know there are many security issues found on MFP devices, with many of these issues being easy to identify and mitigate with some basic configuration changes or changing the devices default password. The real struggle is finding them.

It takes time and effort to test for default or weak passwords or examine the device to see if it was configured to integrate into the business and/or contains configurations that are potentially vulnerable. This is where the automated MFP security testing tool known as Praeda came from.

The original [Praeda](#) tool, written in [Perl](#), was released in 2011 and it first focused on testing for default passwords and checking and exploiting the vulnerabilities that we were aware of at that time. Over time, it has been expanded from just MFP devices to include other embedded devices. In the end, the original Praeda was able to test for default credentials and vulnerabilities on over 120 different MFPs and embedded devices often encountered on corporate networks. Sadly, the original Praeda tool has fallen out of support and has not been maintained for a number of years.

Jump forward to 2024 and an effort to resurrect Praeda and bring it up to date for testing newer MFP devices on the market has begun. That year, we began rewriting Praeda ([Praeda-II](#)). In an attempt to get broader community support we decided to rewrite Praeda-II in the latest version of Python. To start this rebuild project, we also purchased several current-model enterprise MFPs to test out and build a few base modules.



Praeda-II was released on August 7, 2024 at [Blackhat Arsenal](#). The main difference between Praeda and Praeda-II, besides the language it is written in, is the new version will not focus on doing any real vulnerability exploitation, like the original one did. The reason: [Metasploit](#) is the correct tool to be used for exploitation as most of the exploits from Praeda were ported to Metasploit in 2016 and 2017. The goal for Praeda-II moving forward is an auditing tool that can be used as a nonintrusive scanner to identify whether an MFP has configured services and issues that can potentially be exploited and, if so, report that data back. This allows the tool to be used by pentesters, auditors, and IT support teams to make determination about their MFP security posture.

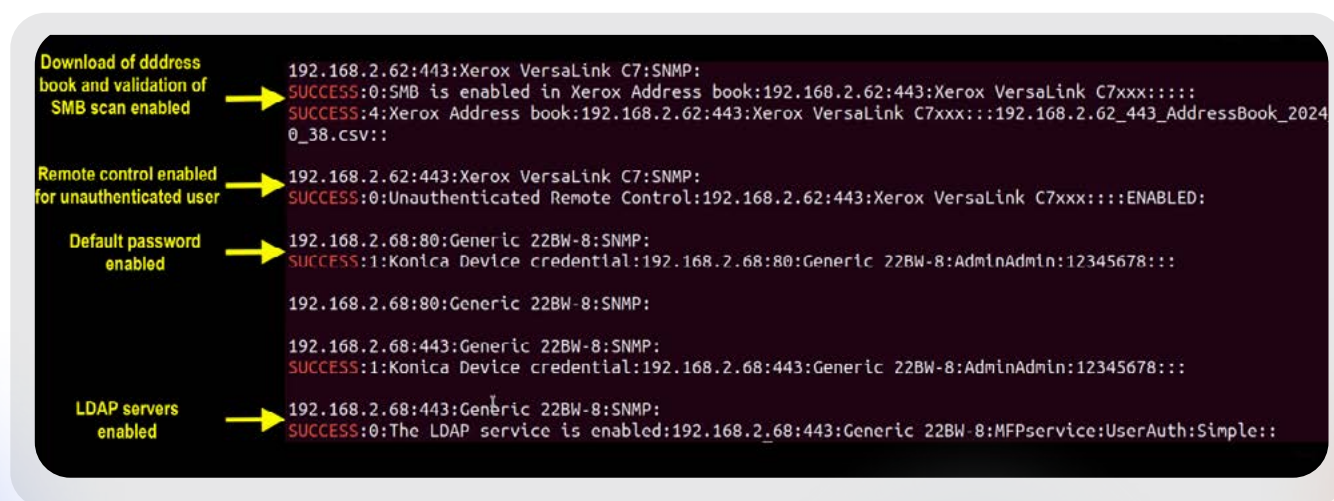


FIGURE 7

Output from Praeda-II showing **potential vulnerable** setting enabled on MFP devices

Even though it has been over a year since the new python version of Praeda-II was released, it is still in its early stages of development. The main engine is done, and modules for several MFP brands including Xerox, Konica, Ricoh, and added fingerprints for many more, have been created. For the Praeda-II project to be successful the community needs to pitch in — pentesters, auditors, and other support organizations — to help build out more modules, fingerprints, and test current modules against various models.

For those interested, there are a few [YouTube](#) videos on how to use the tool and how to set up and create fingerprints. We plan to update and add more how to videos as time permits covering creation of modules and expanding out Praeda-II's capabilities.

Conclusion

Securing MFPs in an enterprise environment requires treating them as first-class network assets rather than peripheral appliances. Best practices begin at the point of acquisition. Organizations should evaluate vendors not just on cost and performance, but also on the maturity of their security posture, including availability of regular firmware updates, support lifecycles, and built-in features such as encrypted storage-and-secure boot.

During deployment, IT teams should immediately replace default or serial-based passwords with strong, unique credentials, disable unnecessary services and protocols, and, when reasonable, place printers on segmented VLANs with limited access.

Logging and monitoring should be enabled from day one to ensure anomalies in printer behavior are detectable, particularly since these devices can be targeted as low-visibility footholds.

Governance is also as important as technical hardening. Enterprises should clearly define ownership of printer security — whether under IT operations, security, or a hybrid model — and establish policies for patch management, configuration baselines, and user access control. Patching and firmware updates should be tracked with the same rigor as operating systems and servers, ensuring timely remediation of critical CVEs.

Regular penetration testing and security audits should include MFPs, not just servers and workstations, to validate defenses and uncover overlooked weaknesses before adversaries can exploit them. Access policies should require authentication for sensitive functions such as scan-to-email or administrative changes, and user training should emphasize that printers are part of the security ecosystem, not exempt from it.

Organizations must plan for the full lifecycle of these devices, from cradle (acquisition and original deployment) to grave (decommission). When an MFP is decommissioned, data remnants on internal hard drives or memory can pose significant leakage risks if not securely wiped. Proper decommission governance helps prevent attackers from recovering sensitive information from discarded hardware.

By integrating MFPs into broader security governance, enforcing strong authentication, maintaining proactive patching, and managing devices responsibly through to retirement, enterprises can turn one of their most overlooked attack surfaces into a well-controlled component of their security posture.

ABOUT RAPID7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open-source communities and cutting-edge research—using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.



SECURE YOUR

Cloud | Applications | Infrastructure | Network | Data

ACCELERATE WITH

[Command Platform](#) | [Exposure Management](#) |
[Attack Surface Management](#) | [Vulnerability Management](#) |
[Cloud-Native Application Protection](#) | [Application Security](#) |
[Next-Gen SIEM](#) | [Threat Intelligence](#) | [MDR Services](#) |
[Incident Response Services](#) | [MVM Services](#)

SECURITY BUILT TO OUTPACE ATTACKERS

Try our security platform risk-free -
start your trial at rapid7.com



© RAPID7 2025 V1.0