Hackers Can Gain Active Directory Privileges Through Vulnerability in Xerox Printers

Hackers Can Gain Active Directory Privileges Through Vulnerability in Xerox Printers

February 18, 2020 BY Securicon Team

Organizations beware: last week, Xerox released a **security advisory** for several models of the WorkCentre Multifunction and Color Multifunction printers. Thanks to a Lightweight Directory Access Protocol (LDAP) vulnerability, hackers can launch a pass-back attack against printers with weak or default credentials. This exposes the login information of Active Directory users – including those with administrative privileges – and can be used to gain further control over an organization's network.

Deral Heiland and Michael Belton's research on multi-function printers and the "Pass-Back Attack" first appeared in **a document published on foofus.net**. Steven Campbell, a Senior Security Consultant at Securicon, frequently finds network devices using default credentials that are vulnerable to the pass-back attack vector during client assessments and uses this attack vector to discover credentials to Active Directory service accounts.

Unfortunately, the newly reported vulnerability in Xerox WorkCentre MFP's is just one in a series of similar weaknesses impacting today's off-the-shelf IoT devices. In this article, we'll explain how it can be used to gain administrative access over Active Directory domains, and what you should do to protect yourself.

How it Works: Xerox Pass-Back Attack

First – after accessing an organization's network – a malicious or unauthorized user can gain access to the Web interface for affected Xerox printers using well-known, default login credentials. Even if the username and passwords have been changed, they may be brute-forced if they are weak and easily guessable.

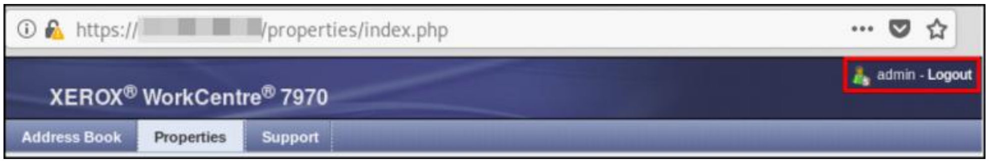
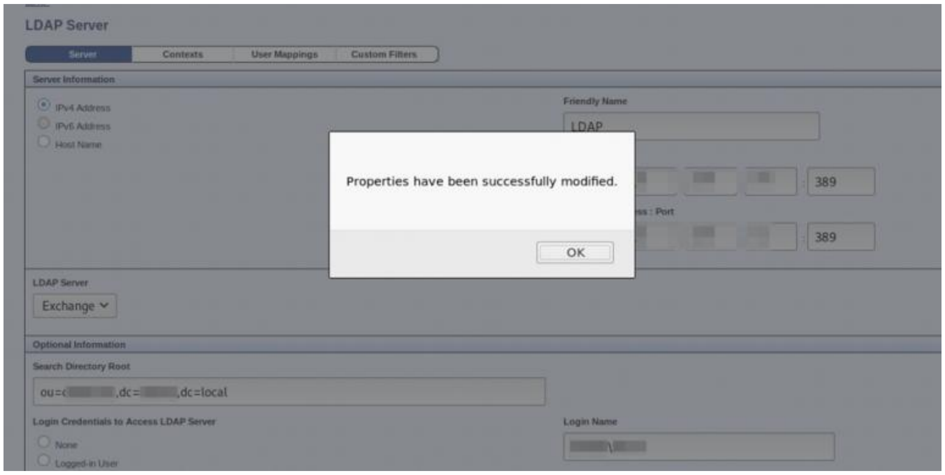


Figure 1: Admin interface accessed using default credentials

Next, the actor finds an LDAP connection configured on the device and changes the Server IP address or hostname to their own IP address as shown in the next figure. Since the Xerox firmware does not require a user to re-enter or validate the LDAP credentials before changing its server address, there is nothing standing in the attacker's way.



LDAP Server

Server Information

● IPv4 Address
○ IPv6 Address
○ Host Name

Friendly Name: LDAP

[redacted] : 389

[redacted]ss : Port

[redacted] : 389

Properties have been successfully modified.

LDAP Server: Exchange

Optional Information

Search Directory Root: ou=[redacted],dc=[redacted],dc=local

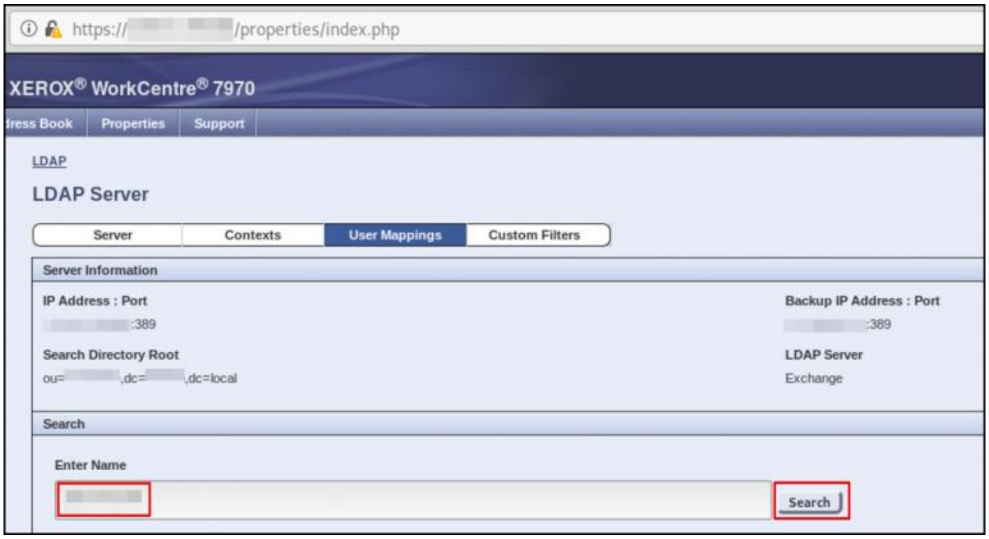
Login Credentials to Access LDAP Server

○ None
○ Logged-in User

Login Name: [redacted]

Figure 2: Editing LDAP Connection

Next, the attacker uses a utility like netcat to listen for incoming connections and display the output in plaintext. Using the LDAP server search field, they can search for any name and connect to the corresponding account.



https://[redacted]/properties/index.php

XEROX® WorkCentre® 7970

LDAP

LDAP Server

Server Information

IP Address : Port
[redacted]:389

Backup IP Address : Port
[redacted]:389

Search Directory Root
ou=[redacted],dc=[redacted],dc=local

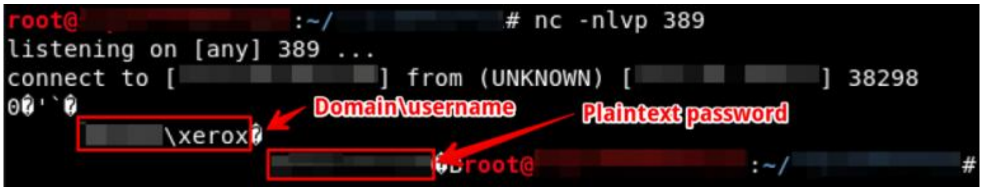
LDAP Server
Exchange

Search

Enter Name: [redacted]

Figure 3: LDAP User Search

On the actor's system, the netcat utility receives the connection and displays credentials used by the printer to reach the Active Directory Domain Controller, including domain, username and password.



```
root@[redacted]:~/[redacted]# nc -nlvp 389
listening on [any] 389 ...
connect to [[redacted]] from (UNKNOWN) [[redacted]] 38298
0�'`�
    [redacted]\xerox�
                [redacted]��root@[redacted]:~/[redacted]#
```

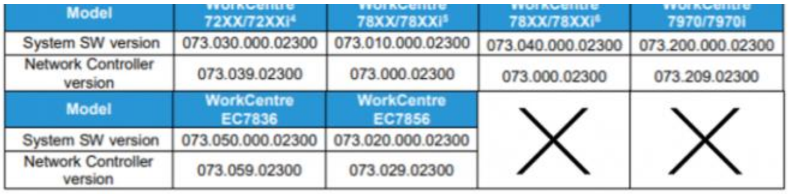
Figure 4: Capturing Plaintext Credentials

In the best-case scenario, the attacker will discover an ordinary Active Directory user account that does not belong to any privileged security groups. The attacker can still use the unauthenticated user to gain a foothold in the domain, which constitutes a moderate vulnerability.

However, our own tests on client networks demonstrate that the worst-case scenario is more likely. We frequently find that the printer service account belongs to a privileged group such as "Domain Admins," and grants the attacker full control over the Active Directory Domain. This is a severe vulnerability which requires immediate remediation.

Are You Protected?

The table below lists Xerox printers susceptible to the attack outlined above, and the corresponding firmware patch. Devices on a lower software version are still vulnerable and should be patched using **the updates** provided by Xerox.



Model	WorkCentre 72XX/72XXi[4]	WorkCentre 78XX/78XXi[5]	WorkCentre 78XX/78XXi[6]	WorkCentre 7970/7970i
System SW version	073.030.000.02300	073.010.000.02300	073.040.000.02300	073.200.000.02300
Network Controller version	073.039.02300	073.000.02300	073.000.02300	073.209.02300
Model	WorkCentre EC7836	WorkCentre EC7856	✗	✗
System SW version	073.050.000.02300	073.020.000.02300		
Network Controller version	073.059.02300	073.029.02300		

Aside from installing the latest firmware update, we recommend that organizations implement two security controls across all their networked devices to prevent similar attacks in the future:

1. Always update default manufacturer credentials with strong passwords and use two-factor authentication (2FA) whenever possible. Recently, **Barracuda network devices** were impacted by an LDAP vulnerability similar to the one described in this article; all users were impacted except for those enrolled in 2FA.
2. System administrators should avoid adding printer service accounts to privileged Active Directory groups, and – in general – they should keep the number of administrative users to an absolute minimum.

Although it should be incumbent on vendors and device manufacturers to validate users before allowing them to change crucial device settings (like LDAP IP address), the truth is that today's vendors cannot be trusted to enforce rigorous security controls. Organizations must take the initiative to strategically protect their networks.

Bridging the IoT Security Gap

In the past, we have talked about the **IoT security gap** and lax controls from hardware manufacturers. Sadly, the vulnerability covered in this article is a case-in-point: today, networked devices are being pushed to market faster than they can be secured, and security is rarely a priority in development. This leaves many organizations with blind spots in their security position as a host of seemingly benign devices (like printers) provide **a wide attack surface** for malicious actors.

IoT and networked devices are the future – but meeting the technological needs of your business and protecting your investment are not mutually exclusive goals. As the **average cost for a data breach** climbs to historical highs, organizations cannot afford to be caught off guard by easily prevented security vulnerabilities. This year insure your organization against future threats by taking inventory of your IT assets and assessing them for risk.

---

*Securicon's **risk management solutions** are based on the industry standards for safety and professionalism. With years of experience in IT and critical infrastructure, we are here to protect your organization and ensure the highest quality of compliance. **Contact us** for more information on our risk assessment framework*

Data Breaches, Hackers, Risk Management