

Upon receiving the firmware files (wr-841n.bin, dcs-8000lh.bin, bare-metal-demo.elf) for this project, the first course of action that was taken was to perform reconnaissance on them, which consisted of searching the internet for product information, such as who developed the product, what the product is, when it was released, and how the device can be obtained or purchased. After gathering this initial information, we conducted further research on the known vulnerabilities to determine what type of exploitable information could be obtained from them.

The first file we performed recon on was the wr-841n.bin, which is for the TP-Link TL-WR841N router. We discovered that this device can no longer be purchased new through Amazon, but it can be purchased used. In addition, we were also able to gather the types of Wifi modes it supports, the security protocols it uses, hardware specifications, [User Manual \(PDF\)](#), [Installation Manual \(PDF\)](#), and other basic release information details. Following our initial product information gathering, we performed a Google search for "TP-Link TL-WR841N vulnerabilities." This search yielded numerous websites detailing known weaknesses within the device's firmware. The most significant weakness is the dropbearpwd Improper Authentication Information Disclosure vulnerability, which allows attackers to expose sensitive information in the httpd service. This information provided a good roadmap as to what we could disclose with a successful attack. Upon further research, we were always able to determine that the "TP-Link" brand has had other devices with known vulnerabilities. In addition, at the beginning of 2025, a group of U.S. lawmakers/senators has requested that the "TP-Link" brand be banned in the United States due to the brand being closely tied to the Chinese Communist Party, and for suspicions of embedding surveillance capabilities into U.S. networks.

<https://industrialcyber.co/critical-infrastructure/us-lawmakers-push-to-ban-tp-link-over-national-security-risks-surveillance-concerns/#:~:text=In%20a%20bicameral%20letter%20the,harmful%20capabilities%20into%20U.S.%20networks.>

We also used noseyparker, which complements tools such as binwalk, file, grep, trufflehog, detect-secrets, etc. This software was able to detect hardcoded passwords, base64 credentials, default configuration passwords, and usernames.

Analysis for wr-841n.bin:

File ID: file returned data

Key findings:

- U-Boot string at 0xD120 U-Boot 1.1.3
- LZMA compressed kernel at 0x10200
- SquashFS root filesystem at 0x100000
- Header pattern: repeating 16-byte blocks at file start — likely firmware table/metadata
- Extraction status: binwalk -Me found components but warned sasquatch extractor missing; some symlinks rewritten for safety during extraction
- Immediate IOCs: MD5 97710bf8ae216d4665c1c89a43eca626; timestamps indicate build date 2022-08-16

- Risk/impact notes: contains full root filesystem — may include credentials, web UI, and device configs (sensitive if exposed)
- Tools used: file, xxd, strings, binwalk, binwalk -Me,
- Nosey Parker used and ran a report that discovered the squashfs-root file system. It found API keys for AWS and GitHub aligned with private keys and tokens. It also found the username of the admin and the password in base 64.

Figure 1.1

```
ayoth@PapaVanWinkle:~/noseyparker$ binwalk -e wr-841n.bin -C ~/wr-841n_extracted
DECIMAL      HEXADECIMAL      DESCRIPTION
-----
53536        0xD120          U-Boot version string, "U-Boot 1.1.3 (Aug 16 2022 -
12:01:12)"
66048        0x10200         LZMA compressed data, properties: 0x5D, dictionary
size: 8388608 bytes, uncompressed size: 2986732 bytes

WARNING: Symlink points outside of the extraction directory: /home/ayoth/wr-841n_
extracted/_wr-841n.bin-0.extracted/squashfs-root-0/etc/passwd -> /var/passwd; cha-
nging link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /home/ayoth/wr-841n_
extracted/_wr-841n.bin-0.extracted/squashfs-root-0/etc/TZ -> /var/tmp/TZ; changin-
g link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /home/ayoth/wr-841n_
extracted/_wr-841n.bin-0.extracted/squashfs-root-0/etc/resolv.conf -> /var/tmp/re-
solv.conf; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /home/ayoth/wr-841n_
extracted/_wr-841n.bin-0.extracted/squashfs-root/etc/passwd -> /var/passwd; chang-
ing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /home/ayoth/wr-841n_
extracted/_wr-841n.bin-0.extracted/squashfs-root/etc/TZ -> /var/tmp/TZ; changing
link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /home/ayoth/wr-841n_
extracted/_wr-841n.bin-0.extracted/squashfs-root/etc/resolv.conf -> /var/tmp/reso-
lv.conf; changing link target to /dev/null for security purposes.
1048576       0x100000         Squashfs filesystem, little endian, version 4.0, co-
mpression:xz, size: 3001844 bytes, 552 inodes, blocksize: 262144 bytes, created:
2022-08-16 04:14:58
```

Figure 1.2

```
ayoth@PapaVanWinkle:~/noseyparker$ noseyparker scan ~/wr-841n_extracted --datastore ~/noseyparker/datastore.np
Scanning content [00:00:00]
Scanned 52.13 MiB from 1,089 blobs in 0 seconds (391.37 MiB/s); 13/13 new matches

Rule          Findings    Matches
Generic Password      11        13

Run the `report` command next to show finding details.
```

Figure 1.3

```
ayoth@PapaVanWinkle:~$ binwalk -Me wr-841n.bin
Scan Time: 2025-10-11 11:43:16
Target File: /home/ayoth/wr-841n.bin
MD5 Checksum: 97710bf8ae216d4665c1c89a43eca626
Signatures: 411

DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----
53536        0xD120          U-Boot version string, "U-Boot 1.1.3 (Aug 16 2022 - 12:01:12)"
66048        0x10200         LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 2986732 bytes

WARNING: Symlink points outside of the extraction directory: /home/ayoth/_wr-841n.bin-4.extracted/squashfs-root-0/etc/passwd -> /var/passwd; changing link target to /dev/null for security purposes.
WARNING: Symlink points outside of the extraction directory: /home/ayoth/_wr-841n.bin-4.extracted/squashfs-root-0/etc/TZ -> /var/tmp/TZ; changing link target to /dev/null for security purposes.
WARNING: Symlink points outside of the extraction directory: /home/ayoth/_wr-841n.bin-4.extracted/squashfs-root-0/etc/resolv.conf --> /var/tmp/resolv.conf; changing link target to /dev/null for security purposes.
WARNING: Symlink points outside of the extraction directory: /home/ayoth/_wr-841n.bin-4.extracted/squashfs-root-0/etc/passwd -> /var/passwd; changing link target to /dev/null for security purposes.
WARNING: Symlink points outside of the extraction directory: /home/ayoth/_wr-841n.bin-4.extracted/squashfs-root-0/etc/TZ -> /var/tmp/TZ; changing link target to /dev/null for security purposes.
WARNING: Symlink points outside of the extraction directory: /home/ayoth/_wr-841n.bin-4.extracted/squashfs-root-0/etc/resolv.conf --> /var/tmp/resolv.conf; changing link target to /dev/null for security purposes.
1048576      0x100000         Squashfs filesystem, little endian, version 4.0, compression:xz, size: 3001844 bytes, 552 inodes, blocksize: 262144 bytes, created: 2022-08-16 04:14:58

Scan Time: 2025-10-11 11:43:17
Target File: /home/ayoth/_wr-841n.bin-4.extracted/10200
MD5 Checksum: 9e838c993a40353342730bb87a432c3
Signatures: 411

DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----
2240608      0x223060         Linux kernel version 2.6.36
2240772      0x223104         CRC32 polynomial table, little endian
2280128      0x222AC0         CRC32 polynomial table, little endian
2280160      0x222B00         xz compressed data
2556368      0x270100         Neighborly text, "NeighborSolicitsInDatagrams"
2556388      0x2701E4         Neighborly text, "NeighborAdVERTISEmentsorts"
2559855      0x270F6F         Neighborly text, "neighbor %2x.%2x.%pM lostname link %s to %s"
2981888      0x208000         ASCII cpio archive (SVR4 with no CRC), file name: "/dev", file name length: "0x00000005", file size: "0x00000000"
2982004      0x208074         ASCII cpio archive (SVR4 with no CRC), file name: "/dev/console", file name length: "0x00000009", file size: "0x00000000"
2982128      0x2080F0         ASCII cpio archive (SVR4 with no CRC), file name: "/root", file name length: "0x00000008", file size: "0x00000000"
2982244      0x208164         ASCII cpio archive (SVR4 with no CRC), file name: "TRAILER!!!", file name length: "0x00000008", file size: "0x00000000"

Scan Time: 2025-10-11 11:43:18
Target File: /home/ayoth/_wr-841n.bin-4.extracted/_10200.extracted/console
MD5 Checksum: d418cd98f80bd204e9000998ecf8427e
Signatures: 411

DECIMAL      HEXADECIMAL      DESCRIPTION
```

Figure 1.4

```
ayoth@PapaVanWinkle:~$ file wr-841n.bin
wr-841n.bin: data
ayoth@PapaVanWinkle:~$ binwalk wr-841n.bin

DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----
53536        0xD120          U-Boot version string, "U-Boot 1.1.3 (Aug 16 2022 - 12:01:1
2)"
66048        0x10200         LZMA compressed data, properties: 0x5D, dictionary size: 83
88608 bytes, uncompressed size: 2986732 bytes
1048576      0x100000         Squashfs filesystem, little endian, version 4.0, compressio
n:xz, size: 3001844 bytes, 552 inodes, blocksize: 262144 bytes, created: 2022-08-16 04:14
:58

ayoth@PapaVanWinkle:~$ xxd -l 256 wr-841n.bin | head
00000000: ff00 0010 0000 0000 fd00 0010 0000 0000 .....
00000010: 0b03 0010 0000 0000 0903 0010 0000 0000 .....
00000020: 0703 0010 0000 0000 0503 0010 0000 0000 .....
00000030: 0303 0010 0000 0000 0103 0010 0000 0000 .....
00000040: ff02 0010 0000 0000 fd02 0010 0000 0000 .....
00000050: fb02 0010 0000 0000 f902 0010 0000 0000 .....
00000060: f702 0010 0000 0000 f502 0010 0000 0000 .....
00000070: f302 0010 0000 0000 f102 0010 0000 0000 .....
00000080: ef02 0010 0000 0000 ed02 0010 0000 0000 .....
00000090: eb02 0010 0000 0000 e902 0010 0000 0000 .....
```

Figure 1.5

```

Finding 5/11 (id d12dd25160c31666593aa775f691eee6fd6271b2)
Rule: Generic Password
Group: Contraseña

Match 1/1 (id 6b27fde3eae8ceee883a0d96a8284cce30190ec4)
File: /home/ayoth/wr-841n_extracted/_wr-841n.bin.extracted/squashfs-root/web/js/language.js
Blob: 6377632166f977511f7123cbcc8b23511af3e4c1 (24586 bytes, text/javascript, unknown charset)
Lines: 1:3378-1:3399

    "Must contain no space(s).",PWD_TIP_LONG:"Must be 6-32 characters long.",PWD_TIP_CHAR:"Must contain at least two types of the following characters: letters, numbers and symbols.",es_MX:{START:"Iniciar",LOGIN:"Iniciar sesión",USERNAME:"Nombre de Usuario",PASSWORD:"Contraseña",NOTE:"NOTA:",MODEL_NO:"Modelo ",TIP_CONFLICT:"TEL router permite que sólo un administrador pueda iniciar sesión al mismo tiempo, por favor intente de nuevo más tarde.",TIP_ERROR:"El nombre de usuario o contraseña es incorrecta, por favor ingrese de nuevo"},TIP_EXCE1:"El nombre de usuario o contraseña es incorrecta, por favor ingrese de nuevo"

Finding 6/11 (id d3a7d5c5be8c807088c881d556c40594c6cafc5d)
Rule: Generic Password
Group: Hasło

Match 1/1 (id 47222cb62d9ce53f40cd90b0ba86855ba2cb82da)
File: /home/ayoth/wr-841n_extracted/_wr-841n.bin.extracted/squashfs-root/web/js/language.js
Blob: 6377632166f977511f7123cbcc8b23511af3e4c1 (24586 bytes, text/javascript, unknown charset)
Lines: 1:11306-1:11322

    "PWD_TIP_SPACE:"공백이 없어야 합니다.",PWD_TIP_LONG:"6-32 자로 해야 합니다.",PWD_TIP_CHAR:"문자, 숫자 및 기호 두 가지 이상을 포함해야 합니다.",pl_PL:{START:"Początek",LOGIN:"Zaloguj",USERNAME:"Nazwa użytkownika",PASSWORD:"Hasło",NOTE:"UWAGA:",MODEL_NO:"Model No.",TIP_CONFLICT:"Tylko jeden administrator może być zalogowany na routerze, sprawdź ponownie później.",TIP_ERROR:"Nazwa użytkownika lub hasło są nieprawidłowe, wprowadź je ponownie.",TIP_EXCE1:"Liczba znaków musi wynosić od 6 do 32."},TIP_EXCE1:"Hasło nie jest prawidłowe, wprowadź je ponownie"

Finding 7/11 (id 51b205ad19d21fe2d108b3fb1d9fc6748da40894)
Rule: Generic Password
Group: Senha

Match 1/1 (id 4a24f97672cfb296b00f49732d8ea2008269e7fa)
File: /home/ayoth/wr-841n_extracted/_wr-841n.bin.extracted/squashfs-root/web/js/language.js
Blob: 6377632166f977511f7123cbcc8b23511af3e4c1 (24586 bytes, text/javascript, unknown charset)
Lines: 1:12703-1:12718

    TIP_SPACE:"Spacje nie są dozwolone.",PWD_TIP_LONG:"Musisz mieć długość 6-32 znaków.",PWD_TIP_CHAR:"Musisz zawierać co najmniej dwa typy następujących znaków: litery, cyfry i symbole.",pt_BR:{START:"Início",LOGIN:"Login",USERNAME:"Nome de usuário",PASSWORD:"Senha",NOTE:"NOTA:",MODEL_NO:"Número do Modelo",TIP_CONFLICT:"O roteador permite apenas um administrador fazendo o login por vez, por favor, tente mais tarde.",TIP_ERROR:"O nome de usuário e senha está incorreto, por favor, tente novamente.",TIP_EXCE1:"Você deve digitar pelo menos 6 e 32 caracteres."},TIP_EXCE1:"Senha inválida ou não foi digitada corretamente"

Finding 8/11 (id 87f074b4d3e40295a12b4ea57a02ca188982f82c)
Rule: Generic Password
Group: Parolă

Match 1/1 (id 59422bd61bbdf26fe0a727c3eb378ea8c79fc9b1)
File: /home/ayoth/wr-841n_extracted/_wr-841n.bin.extracted/squashfs-root/web/js/language.js
Blob: 6377632166f977511f7123cbcc8b23511af3e4c1 (24586 bytes, text/javascript, unknown charset)
Lines: 1:14037-1:14054

    Numele de utilizator și parola trebuie să conțină cel puțin 6 și cel多 32 caractere.",PWD_TIP_LONG:"Deve ter de 6 a 32 caractere.",PWD_TIP_CHAR:"Deve conter pelo menos dois tipos dos seguintes caracteres: letras, números e símbolos.",ro_RO:{START:"Început",LOGIN:"Autentificare",USERNAME:"Nume de utilizator",PASSWORD:"Parolă",NOTE:"NOTA:",MODEL_NO:"Model No.",TIP_CONFLICT:"Routerul permite un singur administrator să fie autentificat simultan, vă rugăm să încercați mai târziu.",TIP_ERROR:"Numele de utilizator sau parola sunt incorrecte, vă rugăm să le introduceți din nou"},TIP_EXCE1:"Parola este înșcrierea nu este corectă sau nu a fost introdusă"

```

Figure 1.6

```

Finding 9/11 (id f223866a043caf1b65d131e7a6f9b9ce25e2946b)
Rule: Generic Password
Group: Password

Match 1/2 (id b6eac29926bbfa630ef5ef3c262c7776cb24f9d4)
File: /home/ayoth/wr-841n_extracted/_wr-841n.bin.extracted/squashfs-root/web/js/language.js
Blob: 6377632166f97751f7123bcc8b23511af3e4c1 (24586 bytes, text/javascript, unknown charset)
Lines: 1:2080-1:2098

    D_TIP_SPACE:"Darf keine Leerzeichen enthalten.",PWD_TIP_LONG:"Muss 6-32 Zeichen lang sein.",PWD_TIP_CHAR:"Muss mindestens zwei Arten von folgenden Zeichen enthalten: Buchstaben, Zahlen und Symbole.",en_US:{START:"Start",LOGIN:"Log In",USERNAME:"Username",PASSWORD:"Password",NOTE:"NOTE:",MODEL_NO:"Model No. ",TIP_CONFLICT:"The device allows only one administrator to login at the same time, please try again later.",TIP_ERROR:"The password is incorrect, please try again.",TIP_EXC1:"You have exceeded ten attempts. Please try again."}

Match 2/2 (id 88dfe13783b79f91856fc864ebc6a19d5d53487a)
File: /home/ayoth/wr-841n_extracted/_wr-841n.bin.extracted/squashfs-root/web/js/str.js
Blob: d2c64c6cf4a0f1b38bcd871d0acf64d35b72e3740 (101898 bytes, text/javascript, unknown charset)
Lines: 1:16397-1:16415

    nable SSID Broadcast",host:"Host",wlScheCtl:"(schedule control)",wlUsrCtl:"(user control)",locale:"Locale Selection",prof:"Profile Name",phone:"Phone Number/User ID",registraraddr:"Registrar Address",registrarport:"Registrar Port",auid:"Authentication ID",password:"Password",sipproxy:"SIP Proxy",sipproxyport:"SIP Proxy Port",outboundproxy:"Outbound Proxy",outboundproxyport:"Outbound Proxy Port",label:"Register via Outbound Proxy",siplist:"SIP Account List",sipaccount:"Voice - SIP Account",blacklistconf:"Black List-Configuration",

Finding 10/11 (id 5cc15c7fd01f881271e3171c94090b3f07ad9d3d)
Rule: Generic Password
Group: Passwort

Match 1/1 (id 384798527bff69970a1ab390b6858bb9d2f47ec5)
File: /home/ayoth/wr-841n_extracted/_wr-841n.bin.extracted/squashfs-root/web/js/language.js
Blob: 6377632166f97751f7123bcc8b23511af3e4c1 (24586 bytes, text/javascript, unknown charset)
Lines: 1:671-1:689

    ,sv_SE:"Svenska",th_TH:"ไทย",tr_TR:"Türkçe",uk_UA:"Українська",vi_VN:"Tiếng Việt",zh_CN:"简体中文",zh_TW:"繁體中文",ar_AR:"عربی";var _localString={de_DE:{START:"Start",LOGIN:"Einloggen",USERNAME:"Benutzername",PASSWORD:"Passwort",NOTE:"Hinweis:",MODEL_NO:"Model No. ",TIP_CONFLICT:"Es kann immer nur ein Teilnehmer in den Router eingeloggt sein. Bitte versuchen Sie es später noch einmal.",TIP_ERROR:"Ungültige Zugangsdaten. Bitte versuchen Sie es noch einmal.",TIP_EXC1:"10 Fehler"}}
```

Finding 11/11 (id 8514bd2a296b459feddbade5a112e7235da16b9)

Rule: Generic Password

Group: admin

```

Match 1/1 (id 0aabf0c6b4b966db54f50047cf2bd7e04cb0ac0d)
File: /home/ayoth/wr-841n_extracted/_wr-841n.bin.extracted/squashfs-root/web/help/RestoreDefaultCfgHelpRpm.htm
Blob: fe7bd6c3a46c0baac327fe34c25fe8d18c3d2382 (2311 bytes, text/html, unknown charset)
Lines: 25:50-25:525
```

```

document.getElementById("defaultPassword").innerHTML+=" - <B>" + (typeof default_password!="undefined"?default_password:"&lt;PS PIN&gt;") + "</B>" }else{document.getElementById("defaultPassword").innerHTML+=" - <B>" + (typeof default_password!="undefined"?default_password:"admin") + "</B>" }if(INCLUDE_US_CPI_SPEC){document.getElementById("defaultIpAddress").innerHTML+=" - <B>" + (typeof default_ip_address!="undefined"?default_ip_address:"192.168.15.15") + "</B>" }else{document.getElementById("defaultIpAddress").innerHTML+=" - <B>" + (typeof
```

The second file we performed recon on was the dcs-8000lh.bin, which is for the D-Link Mini HD WiFi Camera. In comparison to the TP-Link router, this device is still actively sold through [Amazon.com](#) and can be purchased for \$18.95. Similarly, we were able to locate product information on this device, such as the flash memory type, power source, internet connectivity protocol, video capture format, and [User Manual \(PDF\)](#). Following our initial product information gathering, we performed a Google search for "D-Link dcs-8000lh Vulnerabilities." This search resulted in various vulnerabilities and also other known D-Link products that have the same security weakness as the 8000LH. The vulnerability these devices face consists of attackers being able to view the device's configuration file by running the following command: "<Camera-IP>/common/info.cgi" By doing so, attackers can get ahold of the following information from the device: model, brand, version, build, hw_version, nipca_version, device name, location, MAC address, IP address, gateway IP address, wireless status, input/output settings, speaker, and

sensor settings <https://nvd.nist.gov/vuln/detail/cve-2018-18441#match-14738767>. This information would allow for targeted attacks and comes with a low barrier of entry, given that all the attacker would need is the device's IP address. Once that has been obtained, the ability for the device to be immediately controlled by an attacker is significant. After running noseyparker on the DCS-8000lh.bin file, a 2048-bit RSA private key was found along with a https/tls certificate private key, unencrypted with no password protection. This exposes the camera to certificate authentication whomever and camera streams can be accessed.

Analysis for dcs-8000lh.bin

- A 2048-bit RSA private key was found along with a https/tls certificate private key, unencrypted with no password protection.

Figure 2.1

```
ayoth@PapaVanWinkle:~/noseyparker$ noseyparker scan \
--datastore dcs8000lh_scan.db \
_dcs-8000lh.bin.extracted/
Scanning content [00:00:00]
Scanned 56.53 MiB from 795 blobs in 0 seconds (490.39 MiB/s); 1/1 new matches

      Rule          Findings     Matches
-----+-----+-----+
PEM-Encoded Private Key           1            1

Run the `report` command next to show finding details.
ayoth@PapaVanWinkle:~/noseyparker$
```

Figure 2.2

```
ayoth@PapaVanWinkle:~/noseyparker$ noseyparker report --datastore dcs8000lh_scan.db
Finding 1/1 (id 64a9a9d2166f82cd253c747ceaebe8840736d)
Rule: PEM-Encoded Private Key
Group:

MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCO3Dn068+mvF3x
MPIq0/TjqBphazNHwnDKP7sdtX7mr7RBWsVVPAsjXLSFiuhIq9i/rjNvrwPL1e
2v3U3z7g07SkK4e2Y3c2LV++ThJPcqjopA53/UBTmVPUJ04mrEKb211XWSZ/4VE0
RMU07/JP10PyAMNBURBwl7ON7oWoW3q5yP912Lgq/KkP7/KK904xs03BgyVwd
CDAM75x+zNVhzXjFqmrxGu+YwiGLqn2kPPpl552zYdFlmV+bbz7Xmmic66cSTW
wKmzNnxPykL1wfuiLyMyEAZ9w9U0lQysr09s80z689ik8pyTv61UEIIbanPk2E
zteWEz5zAgMBAECCggEBAKgMxF1NzIHbwawYyOpKEfu8VaLVeAVB3PGgPB5DyVF
SS5w6WodzTa0U/xzq48LksEq8wyjyk11Pg5IWtjV4tgG/p9YrzZiv59Ak+kBI/Rc
ZuQbpDILybqlqIXFq9E1WGrOyLfq7ej/FFC8zaPYAn9X3EWrBFxtK24or8SW0FE0
U6qe06Xycf4uu8z+zWdEQpm97bqASVj2kbkKYaxXTJMavxbpnPxIFkfxsu9kCQ5H
Ux0jXZAcD7+Trmp4whPVFQp+QPUi6lhxBUKxdewKQbwKIVeayYmuLfZf2HYg5Es
rDK01PoSNhzV8i1d6z28ctxhPh5GEHf3U6A849MyILkCgYEAs2psxs45tUN6LHxWp
Q+S17VuQInAoM1bTJ2I6dil2n08frauIFUEwaXn1nWifllyn6zUmVKyLgf2d/fuN
d0PBihT7KfNx32nvDMF4p+ex/+uNWsS1l0qqfujGt9bEz007ic+SMx8kH9byA+AE
4Fj40VERD203zTWSGzDoCjaPGK8CgYEAO8w6W0P0jvp+Iq+fW6ou2PI1NKBgapH7
PaZNeE5TUrljIjMqofy3KKhlFSYUfhShoyVATH2bxwKNErKBeCSVcgafJtqiU1e
JJ4dozlFNP+7urVZZw2k5A7TsTbsjVcQTFKcs69tPe5H+jRdpIBt+Ix8QpQsaoB
rFUm9wT5H30CgYAU04on5uWV+H1/6ycclwfsL8ml50TDLJYFT/sEh3f2JrM13li
1v8g10YQyE6RyJb8M5oRAUmRTCwoDfhn3HDbsuwxUFK+7ffty8VecxjJ61DYGChp
G0/Aod1Bz1PA1z0XQ6meuyVEuk0G104+yaCA16xx1xr0F8IqaRcpLK0pGwKBgHba
b5ERjx0rPCdo2IuPB/UUjoj2yuhNPWk0LwEpKxcME7Z4ch8u+vaKve2redp8+aqp
r2Bc+BBeqdyyFmaRjKZr6EIE0Rc1xHPWCzs0duURJYLUBV0m4NZd/6u6WeBDEFFU
Nr2a3znWwquEssTykV3eJOIeAIomDgRQUKpkLwzdAoGANgeyqPWYyZirigJVpzkw
Vkp1eaPOExIz3bBNdxpCGPw3qKysnGTA5M9T0TRaxYC769XVFTZ1YQftdlypT33G
uumEXaV+LNn9H3VK1U4MR1hP5yuWb0wzauPQhLwrrkH05bwElng9CuT8zmvd1HLf
V1c6clJiKhywL3FYyquXx4=
```

Figure 2.3

```
Match 1/1 (id 4e612711302bb2039d694b2c423f20286ead8f7)
File: _dcs-8000lh.bin.extracted/160000
File: _dcs-8000lh.bin.extracted/1A0000
Blob: eddff23dce478af4e7c504c5ec2ccf44bbeeb5b3f (114688 bytes, unknown type, unknown charset)
Lines: 922:10-949:25

    " content="www.dlink.com" />
<Validity type="2" content="3650" />
<KeyLength type="2" content="2048" />
</CertificateReq> <HTTPSPem>
<keyData type="5" content="" />
<crtData type="5" content="" />
<crtData type="5" content="" />
<pemData type="5" content="" />
<-----BEGIN PRIVATE KEY----->
MIIEvQIBADANBgkqhki9w0BAQEFAASCBwggSjAgEAAoIBAQCO3Dn068+mvF3x
MPIq0/TjqpbphazNHWnDKP7sdtxmr7RBwsVVPAgSjXl5Fiuhi9i/rjNrvwPL1e
2v3U3z7g7Sk4eZ3c2LV++ThJpcqjopA53/UBTmVPUJ04mrEKB211XWSZ/4VE0
RMu07/JPJ10PyAM8URBwBL70N7wOlw3q5yP912Lgq/Kkp7/KK904xs03BgyVwd
CDAM75x+zNvhzXjFqmr3xGu+YwiGLqaN2kPPpl5S2zYdFlmV+bzb7Xmmic66cSTw
wKmzNnxpYKliwfuMyEAZw9u0lQXysr09s80z68v9ik8pyTV61UEIbanPk2E
zteWez5zgMBAECggEBAKgMxFInzIHbwawYy0pKEfu8VaLVeAVB3PggPB5DyVF
SS5w6WodzTaOU/xzq48LksEq8wyjyk1lPg5SIWjV4tgG/p9YrzZiv59Ak+kBI/Rc
ZuQbpDI1qIXfq9ElwGr0yLfj7eJ/FFC8zaPYAn9X3EWrBFXTK24or8SW0FE0
U6qe06Xycf4uu8z+zWdQpm97bqASyj2kbkYxaTJMvaxbpnPxFkfxsu9kCQP5H
Ux0jXZACD7+tmp4WhPVFUQ+PQUi6tXBUKxdEwKQbWKIVeAYmlfZF2HYg3Es
rDK01PoShzV8i1d6z28txhPh5GEHT3U6A849MyIlKcgYEAs2psXs4stUN6lHxp
Q+S17VqInAOm1bTj2Idilzno8frauIFUEwaXN1nwIflynn6zUmVkyLgf2d/fuN
d0pB1hT7kfNx32nvDMF4p+ex/+uNWsS1l0qqfuJGt9bz00TiC+SMx8kH9by+A
4Fj40VERd203zTWSGzDoCJaPQK8cgYEAE08w6W0P0jvp+Iq+fW6ou2PI1NKBgqpH7
PaZNeE5TUrlijMqofy3KkrLF5YUfhhShoyVATH2bxwKNErKBeCSvCgAfJtqiU1e
JJ4d0z1fNP7/urVZZW2k5A7TsTBsjVcQTFKcs69tPe5H+jRdpIBt+IxN8pQSaob
rFUmwT5H30CgYAUQ4on5uW+H1/6ycclwfSL8mlls0TDLJYFT/sEh3f2JrMI3li
1v8g10YqE6RyJb8M50RAUmRTCo0fhn3HDbssuwUFk+7ffty8VecxjJ61DYGChP
G0/Aod1Bz1PA1z0XQ6meuYVEuk0G104+yaCA16Xx1r0F81qaRpLk0pGwK8ghba
b5ERjx0rPcd02IuPB/UUoj02yuHNpWk0LwEpKxcME7Z4ch8u+vaKve2redp8+aqp
r2Bc+BBeqdDyFMaRjkZr6EI0Rc1xHPWCz5i0duRJYLUBV0m4Nzd/6u6WeBDEFFU
Nr2a3znwquEssTYkV3j0IeAIomDgRQUPkpLwzdAoGANgeyqPWyYzirigJVpzkw
Vkp1eaPOExIz3bBndXpCGPW3qKySnGTASMT0tRaxYC769xVFTZ1YqfTdypt3G
uumExaV+LnnH3VK1U4MR1hp5yuwb0wauPQhLwRkH05bwElng9CuT8zmvd1HLf
V1c6clJiKhywl3FYyquxx4=
<-----END PRIVATE KEY----->
<pemData2 type="5" content="" />
<-----BEGIN CERTIFICATE----->
MIIDzTCARwgaIBAgIAj01egRVfJA40MA0GCSqGSIb3DQEBCwUAMH0xCzAJBgNV
BAYTAlRXM0wCwYDVQQIDARBc2lhMQ0wCwYDVQQHDARBc2lhMRswGQYDVQKDBJE
LUxpbmsgQ29ycG9yYXRpb24xGzAZBgnVBAsMEkQtTGluaYBDb3Jwb3JhdGlvbjEW
```

Analysis for bare-metal-demo.elf

- ELF 32-bit LSB executable, ARM, EABI5
- AWS access and secret key, GitHub Auth token, and personal access token, along with a PEM private key

Automation Script

In technology, establishing routine patterns and building in automation is almost always preferred. By doing so, it provides efficiency and also higher levels of accuracy, which is extremely important when trying to detect potential software vulnerabilities. That said, we developed a Python script to help in the analysis of .bin and .elf firmware images by automating the extraction and scanning of hardcoded secrets.

The script we built has two main capabilities. For .bin files, the script invokes binwalk, which is a firmware analysis tool that helps detect squashfs file systems that are usually stored on Linux IoT devices. That said, the script we developed looks to see if a

Squashfs file system is on the device; if it is, the location is stored for further review. Regarding the .elf file, we chose to use the software noseyparker, which was developed by Praetorian, to assist in the detection of stored secrets and sensitive data. Each time this script runs, noseyparker creates a temporary datastore to isolate the extracted data from the .elf file. This datastore is then used later to discover hardcoded secrets, such as passwords, tokens, and SSH keys.

Our method of execution for this script was in VS Code, which provides a user-friendly UI for executing scripts and viewing folders and files in a centralized location. This entire script runs in a few seconds and produces folders with extraction files for each .bin file and an overall findings.json file that contains the vulnerabilities it was able to discover. The vulnerabilities for the .elf file are also stored in the same .json file. As previously mentioned, the time savings and ability to view all vulnerability findings in a single location are the benefits of building out an automation script.

Figure 3.1