

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. Please refer to all screenshots in the Git repository for the initial reconnaissance performed on the files.

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%2C%20the.harmful%20capabilities%20into%20U.S.%20networks."](https://industrialcyber.co/critical-infrastructure/us-lawmakers-push-to-ban-tp-link-over-national-security-risks-surveillance-concerns/#:~:text=In%20a%20bicameral%20letter%2C%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; 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-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_extracted/_wr-841n.bin-0.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_extracted/_wr-841n.bin-0.extracted/squashfs-root/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_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/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
---------	----------	---

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/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/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/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, blocksiz
e: 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:  9e83bc993a40353442730b887a432c3
Signatures:     411
-----
DECIMAL      HEXADECIMAL    DESCRIPTION
-----
2240608      0x223060        Linux kernel version 2.6.36
2240772      0x223104        CRC32 polynomial table, little endian
2280128      0x22C4C0        CRC32 polynomial table, little endian
2509588      0x264B14        xz compressed data
2556368      0x2701D0        Neighborly text, "NeighborsSolicits6InDatagrams"
2556388      0x2701E4        Neighborly text, "NeighborAdvertisementsorts"
2559855      0x2709F0        Neighborly text, "Neighbor %s,zx:2x,%M lostrename link %s to %s"
2081888      0x208000        ASCII cpio archive (SVR4 with no CRC), file name: "/dev", file name length: "0x00000005", file size: "0x00000000"
2982004      0x2D8074        ASCII cpio archive (SVR4 with no CRC), file name: "/dev/console", file name length: "0x0000000D", file size: "0x00000000"
2982128      0x2D80F0        ASCII cpio archive (SVR4 with no CRC), file name: "/root", file name length: "0x00000006", file size: "0x00000000"
2982244      0x2D8164        ASCII cpio archive (SVR4 with no CRC), file name: "TRAILER!!!", file name length: "0x0000000B", 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:  d41d8cd98f00b204e9800998ecf8427e
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 - 12:01:12)"
66048        0x10200        LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 2986732 bytes
1048576      0x100000        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 3001844 bytes, 552 inodes, blocksiz
e: 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 .....
ayoth@PapaVanWinkle:~$ binwalk -Me wr-841n.bin

```

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 t
wo types of the following characters: letters, numbers and symbols.{}",es MX:{START:"Iniciar",LOGIN:"Iniciar sesión",US
ERNAME:"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 nombr
e de usuario o contraseña es incorrecta, por favor ingrese de nu

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

0.",PWD_TIP_SPACE:"공백 이 없 어 야 합 니 다 .",PWD_TIP_LONG:"6-32 자 르 해 야 합 니 다 .",PWD_TIP_CHAR:"문 자 , 숫 자 및 기
호 중 두 가 지 이 상 을 포 함 해 야 합 니 다 .",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, sp
róbuj ponownie później.",TIP_ERROR:"Nazwa użytkownika lub hasło są nieprawidłowe, wprowadź je ponownie.",TIP_EXCE1:"Li
mit dziesięciu

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

Match 1/1 (id 4a24f97672cfeb296b00f49732d8ea2008269e7fa)
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:"Musi mieć długość 6-32 znaków.",PWD_TIP_CHAR:"Musi zawierać
co najmniej dwa typy następujących znaków: litery, cyfry i symbole.{}",pt_BR:{START:"Início",LOGIN:"Login",USERNAME:"N
ome 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 incorre
to, por favor, tente novamente.",TIP_EXCE1:"Você

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

Não deve conter espaços.",PWD_TIP_LONG:"Deve ter de 6 a 32 caracteres.",PWD_TIP_CHAR:"Deve conter pelo menos d
ois tipos dos seguintes caracteres: letras, números e símbolos.{}",ro_RO:{START:"Început",LOGIN:"Autentificare",USERNAM
E:"Nume de utilizator",PASSWORD:"Parolă",NOTE:"NOTĂ:",MODEL_NO:"Model No. ",TIP_CONFLICT:"Routerul permite un singur a
dministrator să fie autentificat simultan, vă rugăm să încercați mai târziu.",TIP_ERROR:"Numele de utilizator sau paro
la sunt incorect, vă rugăm să le introduceți din

```

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: 6377632166f977511f7123cbcc8b23511af3e4c1 (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_EXCE1:"You have exceeded ten attempts. Please try ag

Match 2/2 (id 88dfe13783b79f91856fc864ebc6a19d5d53487a)
File: /home/ayoth/wr-841n_extracted/_wr-841n.bin.extracted/squashfs-root/web/js/str.js
Blob: d2c64c6cf4a0f1b38cd871d0acf64d35b72e3740 (101898 bytes, text/javascript, unknown charset)
Lines: 1:16397-1:16415

nable SSID Broadcast",host:"Host",wlscheCtl:"(schedule control)",wlsrCtl:"(user control)",locale:"Locale Selection",prof:"Profile Name",phone:"Phone Number/User ID",registraraddr:"Registrar Address",registrarport:"Registrar Port",aid:"Authentication ID",password:"Password",sipproxy:"SIP Proxy",sipproxyport:"SIP Proxy Port",outboundproxy:"Outbound Proxy",outboundproxyport:"Outbound Proxy Port",label1:"Register via Outbound Proxy",splist:"SIP Account List",sipaccount:"Voice - SIP Account",blacklistconf:"Black List-Configurat

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

Match 1/1 (id 384798527bfff69970a1ab390b6858bb9d2f47ec5)
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: 1:671-1:689

,sv_SE:"Svenska",th_TH:"ภาษาไทย",tr_TR:"Türkçe",uk_UA:"Українська",vi_VN:"Tiếng Việt",zh_CN:"简体中文",zh_TW:"繁體中文",ar_AR:"عربي";var localString={de_DE:{START:"Start",LOGIN:"Einloggen",USERNAME:"Benutzername",PASSWORD:"Password",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 Fehlvers

Finding 11/11 (id 8514bd2a296b459fedddbade5a112e7235da16b9)
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: 25:510-25:525

document.getElementById("defaultPassword").innerHTML+=< - <B>"+(typeof default_password!="undefined"?default_password:"&lt;wps 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](https://www.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, nipa_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 64a9a9d2166f82cd252f53c747ceaeef8840736d)
Rule: PEM-Encoded Private Key
Group:

MIEEvQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQC03Dn068+mvF3x
MPIq0/TjqBphazNHwDKP7sdtX7mr7RBWsVVPaQsJxL5FihIq9i/rjNvrwPL1e
2v3U3z7g07SkK4e2Y3c2LV++ThJPcqjopA53/UBTmVPUJ04mrEKB211XWSZ/4VE0
RMu07/JPJ10PYaMN8URBwBL70N7oWoW3q5yP912Lgq/KkP7/KK904xso3BgyVwWd
CDAM75x+zNVhzXjFqmr3xGu+YwiGLqaN2kPPpL5S2zYdFlmV+bbz7Xmmic66cSTW
wKmzNnxPyKl1wfuILyMyEaZ9w9U0lQXysr09s80z68y9ik8pyTV61UEIIBanPk2E
zteWEz5zAgMBAECCggEBAKGMxXF1NzIHbawYyOpKEfu8ValVeAVB3PGGPB5DyVF
SS5w6WodzTaOu/xzq48lKsEq8wjyykI1PgSIWTjV4tgG/p9YrzZlvS9Ak+kBI/Rc
ZuQbpDILyBylqIXFq9E1WGrOyLfj7ej/FFC8zaPYAn9X3EwrBFXTk24or8SW0FE0
U6qe06Xycf4uu8z+zWdEQpm97bqASvj2kbbKYaXTJMvaxbpnPxFkfxsu9KQP5H
Ux0jXZAcD7+Trmp4WhPVFUQP+QPUI6ihXBUXdEwKQbWKIVeayYmuLfZF2HYg5Es
rDK01PoSNhZV8i1d6z28ctxhPh5GEHf3U6A849MyILkCgYEA2psXs4StUN6lHxwp
Q+S17VuQInA0m1bTJ2I6dIl2n08frouFUEwaXN1nwifLlyn6zUmVKyLgf2d/fuN
dOPBihT7KfNx32nvDMF4p+ex/+uNwsS1l0qgfujGt9bEz00TiC+SMx8KH9byA+AE
4Fj40VERd203zTWSGzDoCJaPGK8CgYEA08w6W0P0jvp+Iq+fw6ou2PI1NKBgqPH7
PaZNeE5TurljIjMqofy3KkHLF5YUfhShoyVATH2bXwKNErKBeCSvCgAfJtqiU1e
JJ4d0zLfnP/7urVZZW2k5A7TsTBsjVcQTFKcs69tPe5H+jRDpIBt+Ixn8QpQSaoB
rFum9wT5H30CgYAUQ4on5uWv+H1/6yccLwFSL8mLL50TDLJYFT/sEh3f2JrMI3li
1v8g10YQyE6RyJb8M5oRAUmrTCoDfhn3HDbsuwXUfK+7ffty8VecxjJ61DYGCHp
G0/Aod1Bz1PA1z0XQ6meuYVEuk0G104+yaCA16Xx1xr0F8IqaRcpLK0pGwKBgHba
b5ERjx0rPCdo2IuPB/UUjoj2yuhNPwk0LwEpKxcME7Z4ch8u+vaKve2redp8+aqp
r2Bc+BBegDdyfMaRjKZr6EIE0Rc1xHPWCzs10dURJYlUBV0m4NZd/6u6WeBDEFFU
N2a3znwWquEssTykV3eJ0IEAIomDgRQUPkLwzdAoGANGeqyqPWyZr1gJVpzkW
Vkp1EaP0EXIZ3b8NdXpCGPW3qKySngTA5M9T0tRAXYC769XvFTZ1YQfTdLypT33G
uumEXaV+Lnn9H3VklU4MR1hP5yuWb0wzauPqHLWwRkH05bWEIng9CuT8zmvd1HLf
V1c6cLJikhywL3FYyquXxX4=
```

Figure 2.3

```
Match 1/1 (id 4e612711302bb2039d694b2c423f20286ead8f7)
File: _dcs-8000lh.bin.extracted/160000
File: _dcs-8000lh.bin.extracted/1A0000
Blob: ecdff23dce478af4e7c504c5ec2ccf44bbe5b3f (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="" />
<csrData type="5" content="" />
<crtData type="5" content="" />
<pemData type="5"
content="-----BEGIN PRIVATE KEY-----
MIIEVQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQC03Dn068+mvF3x
MPiQ0/TjqBphazHHwnDKP7sdtX7mr7RBWsVVPaQsJxL5Fiuhi9i/rjNvrwPL1e
2v3U3z7g075kK4e2Y3c2LV++ThJPcqjopA53/UBTmVPUJ04mrEKB211XWSZ/4VE0
RMu07/JPJ10PYaMNBURBwB170N7oW03qSyP912Lgq/KkP7/KK904xs03BgyVwWd
CDAM75+xzNVhzXjFqmr3xGu+YwiGLqaN2kPPpL5S2zYdFLmV+bbz7Xmmic66cSTW
wKmzNnxPyK1lwFuilyMyEAZ9w9U0LQXysr09s80z68v9ik8pyTV61UEIIBanPk2E
zteWEz5zAgMBAAECCggEBAKgmXf1NzIHbwawYy0pKEfu8VaLVeAVB3P6gPB5DyVF
SS5w6WodzTa0U/xzq48LksEq8WjyykI1PgSIWtjV4tgG/p9YrzZivS9Ak+kBI/Rc
ZuQbp0ILyBylqIXFq9E1WGr0yLFj7ej/FFC8zaPYAn9X3EWRBFXtK24or8S0FE0
U6qe06Xycf4uu8z+zWdEQpm97bqASvj2kbbKYaXTJMvaxbnpPxIFkfxsu9kCQP5H
Ux0jXZACD7+Trmp4WhPVFUQP+QPUi6ihXBUXdEwKQbWKIvEayYmulfZF2HYG5Es
rDK01PoSNhZV8i1d6z28ctxhPh5GEHf3U6A849MyILkCgYEA2psXs4StUN6lHxwp
Q+S17VuQInA0m1bTJ2I6d12n08fFrauIFUEwaXN1nw1fLlyn6zUmVKyLgf2d/fuN
d0PBhT7KfNx32nvDMF4p+ex/+uNWsS1l0qqfujgt9bEz00TiC+SMx8KH9byA+AE
4Fj40VERd203zTWSGzDoCJaPGK8CgYEA08w6W0P0jvp+Iq+fw6ou2PI1NKBgqPH7
PaZNe5TUrljIjMqofy3KkhLF5YUfhShoyVATH2bXwKNErKBeCSvcGafJtqiU1e
JJ4d0zLFNP/7urVZZW2k5A7TsTBsjVcQTfKcs69tPe5H+jRDPiBt+Ixn8QpQsaoB
rFUm9wTSH30CG/AUQ4on5uWvH1/6ycclwFSL8mll50TDLJYFT/seh3f2JrMI3li
1v8g10YQyE6RyJb8M5oRAUmRTcwoDfh3HDbsuwXUfK+7ffty8VecxjJ61DYGCp
G0/Aod1Bz1PA1z0XQ6meuYVEuk0G104+yaCA16Xx1xr0F8IqaRcpLK0pGwKBgHba
b5ERjx0rPCdo2IuPB/UUjo2yuhNPwk0LwEpKxcME7Z4ch8u+vAKve2redp8+aqp
r2Bc+BBegDdyFMaRjKZr6EIE0Rc1xHPWCzSiodURJYLUBV0m4NZd/6u6wEBDEFFU
Nr2a3znWwQuesSTYkV3eJ0IeAIomDgRQUKpkLwzAoGANGeyqPWYyZirigJVPzkW
Vkp1EaP0eXIZ3bBNdXpCGPW3qKySnGTA5M9T0tRAXYC769XvFTZ1YQfTdlypT33G
uumEXaV+LNn9H3VK1U4MR1hP5yuwb0wzauPqHLWwRh05bWEln9CuT8zmvdlHLf
V1c6clJiKhywL3FYyquXx4=
-----END PRIVATE KEY-----" />
<pemData2 type="5"
content="-----BEGIN CERTIFICATE-----
MIIDzTCCArWgAwIBAgIJJA01egRVfJA40MA0GCSqGSIb3DQEBCwUAMH0xChAJBgNV
BAYTA1RlXMQ0wCwYDVQQIDARBC2lhmQ0wCwYDVQQHDAARBc2lhmRswGgYDVQQDBJE
LUXpbmsqQ29ycG9yYXRpb24xGzAZBgNVBAsMEkQtTGLuayBDb3Jwb3JhdGlvbJVEw
```

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

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.

[illegible]