Details of Static Analysis Findings

1. Admin Passwords

The credentials of admin accounts are stored in /etc/shadow or /etc/passwd files in the device OS. Acquiring these admin credentials can enable an attacker to login remotely from anywhere. The following admin passwords have been extracted from the router's firmware under examination:

How to patch?

They should not pre-exist if they exist then they must be present in hashed form. Else, they should be generated during configuration.

Findings

1. media/ext_firm/squashfs-root/etc/shadow
2. media/ext_firm/squashfs-root/etc/passwd
3. media/ext_firm/squashfs-root/bin/passwd
4. media/ext_firm/squashfs-root/bin/mkpasswd
5. media/ext_firm/squashfs-root/sbin/chpasswd

2. SSL Certificates and Private Keys

Most of the vendors have included pre-generated self-signed SSL certificates in the hard coded form in the router's firmware, instead of generating them at the runtime. Some firmware binaries also includes private key in unencrypted PEM format, which can lead to serious security threats. By gaining access of these signed SSL certificates and private keys, HTTPS traffic can be decrypted. Moreover, man in the middle attack is also possible. Listed below are the extracted SSL certificates and keys:

How to patch?

Privileges must be handled carefully on such file. Moreover, access should only have with the root users..

Findings

1. media/ext_firm/squashfs-root/etc/server.pem
2. media/ext_firm/squashfs-root/bin/showkey
3. media/ext_firm/squashfs-root/bin/dropbearkey

3. Configuration Files

Configuration files are critical as they contain authentication secret files, root directory of documents, and user admin details. We observed that in the majority of the cases, web servers run under as the root privileged user, which is a sign of risky configuration and design. Due to these issues, the security of the router's device can be compromised if any of the web components are found vulnerable. Extracted web configuration files and other configuration files are enumerated below:

How to patch?

Configuration files must not be present in plain text.

Findings

1. media/ext_firm/squashfs-root/etc/inetd.conf
2. media/ext_firm/squashfs-root/etc/snmpdv3.conf
3. media/ext_firm/squashfs-root/etc/sysctl.conf
4. media/ext_firm/squashfs-root/etc/snmpd.conf
5. media/ext_firm/squashfs-root/etc/resolv.conf
6. media/ext_firm/squashfs-root/etc/nsswitch.conf
7. media/ext_firm/squashfs-root/etc/wireless/wpa_supplicant_scan.conf
8. media/ext_firm/squashfs-root/etc/udev/udev.conf
9. media/ext_firm/squashfs-root/etc/rc.d/rc.conf

10. media/ext_firm/squashfs-root/etc/default/cf_warn.conf
11. media/ext_firm/squashfs-root/etc/default/wpa_supplicant_infra.conf
12. media/ext_firm/squashfs-root/etc/default/cf_misc.conf
13. media/ext_firm/squashfs-root/etc/default/cf_wireless.conf
14. media/ext_firm/squashfs-root/etc/default/cf_port.conf
15. media/ext_firm/squashfs-root/etc/default/cf_sys.conf
16. media/ext_firm/squashfs-root/etc/default/wpa_supplicant_adhoc.conf

4. Malicious Patterns

If malicious patterns exist then the session between the client and server are not encrypted without a workaround. Therefore, those with access to the TCP/IP packet flow between hosts can observe all the traffic, listen in, and record potentially sensitive information like logins and passwords of users connecting to the servers. In depth search against the malicious patterns highlighted in the tested router's firmware files based upon the vulnerabilites database are given below:

How to patch?

Kerberos protocol should be used and Kerberos can essentially be layered over telnet communication inorder to verify the identity while avoiding login information exploitation.

Findings

1. upgrade

1. media/ext_firm/squashfs-root/etc/wireless/bdiff
2. media/ext_firm/squashfs-root-0/bin/eventd
3. media/ext_firm/squashfs-root-0/bin/console
4. media/ext_firm/squashfs-root-0/bin/webs
5. media/ext_firm/squashfs-root-0/lib/libupgradeFirmware.so
6. media/ext_firm/squashfs-root-0/lib/libsystem.so

2. admin

1. media/ext_firm/squashfs-root/etc/passwdDefault
2. media/ext_firm/squashfs-root/etc/shadowDefault
3. media/ext_firm/squashfs-root-0/bin/console
4. media/ext_firm/squashfs-root-0/bin/webs
5. media/ext_firm/squashfs-root-0/bin/utcpdump
6. media/ext_firm/squashfs-root-0/lib/libconfig.so
7. media/ext_firm/squashfs-root-0/lib/libsystem.so

3. root

1. media/ext_firm/21B1.lzo
2. media/ext_firm/15C3A5.gz
3. media/ext_firm/squashfs-root/etc/inetd.conf
4. media/ext_firm/squashfs-root/etc/passwdDefault
5. media/ext_firm/squashfs-root/etc/group
6. media/ext_firm/squashfs-root/etc/wireless/mboxping
7. media/ext_firm/squashfs-root/etc/udev/rules.d/50-udev-default.rules
8. media/ext_firm/squashfs-root/etc/rc.d/init.d/mdev
9. media/ext_firm/squashfs-root/etc/groupDefault
10. media/ext_firm/squashfs-root/etc/shadowDefault
11. media/ext_firm/squashfs-root/bin/busybox
12. media/ext_firm/squashfs-root/root/dev.tar
13. media/ext_firm/squashfs-root/sbin/brctl
14. media/ext_firm/squashfs-root/sbin/dropbear

15. media/ext_firm/squashfs-root/lib/libip6tc.so.0.0.0
16. media/ext_firm/squashfs-root/lib/libip4tc.so.0.0.0
17. media/ext_firm/squashfs-root/lib/libcrypto.so.1.0.0
18. media/ext_firm/1FD4.lzo
19. media/ext_firm/squashfs-root-0/local/sbin/snmpd
20. media/ext_firm/squashfs-root-0/local/lib/libnetsnmpagent.so.25.0.1
21. media/ext_firm/squashfs-root-0/man/man8/ifrename.8
22. media/ext_firm/squashfs-root-0/man/man8/iwlist.8
23. media/ext_firm/squashfs-root-0/bin/lrz
24. media/ext_firm/squashfs-root-0/bin/wpa_supplicant
25. media/ext_firm/squashfs-root-0/bin/console
26. media/ext_firm/squashfs-root-0/bin/webs
27. media/ext_firm/squashfs-root-0/include/wireless.h
28. media/ext_firm/squashfs-root-0/lib/libupgradeFirmware.so

4. password

1. media/ext_firm/squashfs-root/etc/wireless/wpa_supplicant_scan.conf
2. media/ext_firm/squashfs-root/etc/default/cf_sys.conf
3. media/ext_firm/squashfs-root/bin/dbclient
4. media/ext_firm/squashfs-root/bin/busybox
5. media/ext_firm/squashfs-root/sbin/dropbear
6. media/ext_firm/squashfs-root/lib/libc-2.11.1.so
7. media/ext_firm/squashfs-root/lib/libcrypto.so.1.0.0
8. media/ext_firm/squashfs-root/lib/libc.so.6
9. media/ext_firm/squashfs-root-0/local/lib/libnetsnmp.so.25.0.1
10. media/ext_firm/squashfs-root-0/man/man8/iwconfig.8
11. media/ext_firm/squashfs-root-0/bin/eventd
12. media/ext_firm/squashfs-root-0/bin/wpa_supplicant
13. media/ext_firm/squashfs-root-0/bin/console
14. media/ext_firm/squashfs-root-0/bin/portd
15. media/ext_firm/squashfs-root-0/bin/wpa_cli
16. media/ext_firm/squashfs-root-0/bin/webs
17. media/ext_firm/squashfs-root-0/lib/libsystem.so

5. passwd

1. media/ext_firm/squashfs-root/etc/rc.d/rc.local
2. media/ext_firm/squashfs-root/etc/default/cf_sys.conf
3. media/ext_firm/squashfs-root/bin/busybox
4. media/ext_firm/squashfs-root/lib/libnss_nisplus.so.2
5. media/ext_firm/squashfs-root/lib/libnss_compat.so.2
6. media/ext_firm/squashfs-root/lib/libnss_files.so.2
7. media/ext_firm/squashfs-root/lib/libnss_compat-2.11.1.so
8. media/ext_firm/squashfs-root/lib/libnss_hesiod-2.11.1.so
9. media/ext_firm/squashfs-root/lib/libc-2.11.1.so
10. media/ext_firm/squashfs-root/lib/libnss_files-2.11.1.so
11. media/ext_firm/squashfs-root/lib/libnss_nis-2.11.1.so
12. media/ext_firm/squashfs-root/lib/libnss_nisplus-2.11.1.so
13. media/ext_firm/squashfs-root/lib/libnss_hesiod.so.2
14. media/ext_firm/squashfs-root/lib/libc.so.6
15. media/ext_firm/squashfs-root/lib/libnss_nis.so.2
16. media/ext_firm/squashfs-root-0/local/lib/libnetsnmpagent.so.25.0.1
17. media/ext_firm/squashfs-root-0/bin/webs
18. media/ext_firm/squashfs-root-0/include/wireless.h

19. media/ext_firm/squashfs-root-0/lib/libconfig.so
20. media/ext_firm/squashfs-root-0/lib/libupgradeFirmware.so

6. pwd

1. media/ext_firm/21B1.lzo
2. media/ext_firm/15C3A5.gz
3. media/ext_firm/1DAAEC.squashfs
4. media/ext_firm/squashfs-root/bin/busybox
5. media/ext_firm/squashfs-root/lib/libnss_nisplus.so.2
6. media/ext_firm/squashfs-root/lib/libnss_compat.so.2
7. media/ext_firm/squashfs-root/lib/libnss_files.so.2
8. media/ext_firm/squashfs-root/lib/libnss_compat-2.11.1.so
9. media/ext_firm/squashfs-root/lib/libnss_hesiod-2.11.1.so
10. media/ext_firm/squashfs-root/lib/libc-2.11.1.so
11. media/ext_firm/squashfs-root/lib/libnss_files-2.11.1.so
12. media/ext_firm/squashfs-root/lib/libnss_nis-2.11.1.so
13. media/ext_firm/squashfs-root/lib/libnss_nisplus-2.11.1.so
14. media/ext_firm/squashfs-root/lib/libnss_hesiod.so.2
15. media/ext_firm/squashfs-root/lib/libc.so.6
16. media/ext_firm/squashfs-root/lib/libnss_nis.so.2
17. media/ext_firm/1FD4.lzo
18. media/ext_firm/squashfs-root-0/man/man5/iftab.5
19. media/ext_firm/squashfs-root-0/bin/webs

7. dropbear

1. media/ext_firm/squashfs-root/etc/inetd.conf
2. media/ext_firm/squashfs-root/etc/rc.d/rcS
3. media/ext_firm/squashfs-root/bin/dropbearconvert
4. media/ext_firm/squashfs-root/bin/dbclient
5. media/ext_firm/squashfs-root/bin/dropbearkey
6. media/ext_firm/squashfs-root/sbin/dropbear

8. ssl

1. media/ext_firm/21B1.lzo
2. media/ext_firm/6FBB10.squashfs
3. media/ext_firm/15C3A5.gz
4. media/ext_firm/1DAAEC.squashfs
5. media/ext_firm/squashfs-root/lib/libssl.so.1.0.0
6. media/ext_firm/squashfs-root/lib/libcrypto.so.1.0.0
7. media/ext_firm/1FD4.lzo
8. media/ext_firm/squashfs-root-0/bin/ssl_init
9. media/ext_firm/squashfs-root-0/bin/eventd
10. media/ext_firm/squashfs-root-0/bin/wpa_supplicant
11. media/ext_firm/squashfs-root-0/bin/console
12. media/ext_firm/squashfs-root-0/bin/webs
13. media/ext_firm/squashfs-root-0/lib/libsystem.so

9. private key

1. media/ext_firm/squashfs-root/bin/dropbearconvert
2. media/ext_firm/squashfs-root/bin/dropbearkey
3. media/ext_firm/squashfs-root/lib/libssl.so.1.0.0
4. media/ext_firm/squashfs-root/lib/libcrypto.so.1.0.0
5. media/ext_firm/squashfs-root-0/bin/wpa_supplicant

6. media/ext_firm/squashfs-root-0/bin/console
7. media/ext_firm/squashfs-root-0/bin/wpa_cli
8. media/ext_firm/squashfs-root-0/bin/webs
9. media/ext_firm/squashfs-root-0/lib/libsystem.so

10. telnet

1. media/ext_firm/squashfs-root/etc/inetd.conf
2. media/ext_firm/squashfs-root/etc/services
3. media/ext_firm/squashfs-root/etc/rc.d/rcS
4. media/ext_firm/squashfs-root/bin/busybox
5. media/ext_firm/squashfs-root/lib/libcrypto.so.1.0.0
6. media/ext_firm/squashfs-root-0/bin/console
7. media/ext_firm/squashfs-root-0/bin/webs

11. telnetd

1. media/ext_firm/squashfs-root/etc/inetd.conf
2. media/ext_firm/squashfs-root/etc/inittab
3. media/ext_firm/squashfs-root/bin/busybox

12. secret

1. media/ext_firm/squashfs-root/bin/dropbearkey
2. media/ext_firm/squashfs-root/lib/libssl.so.1.0.0

13. pgp

1. media/ext_firm/21B1.lzo
2. media/ext_firm/15C3A5.gz
3. media/ext_firm/1DAAEC.squashfs
4. media/ext_firm/squashfs-root/lib/libresolv.so.2
5. media/ext_firm/squashfs-root/lib/libresolv-2.11.1.so
6. media/ext_firm/1FD4.lzo

14. gpg

1. media/ext_firm/21B1.lzo
2. media/ext_firm/6FBB10.squashfs
3. media/ext_firm/15C3A5.gz
4. media/ext_firm/1DAAEC.squashfs
5. media/ext_firm/1FD4.lzo

15. token

1. media/ext_firm/squashfs-root/etc/wireless/mboxping
2. media/ext_firm/squashfs-root/bin/busybox
3. media/ext_firm/squashfs-root/lib/ld-linux.so.3
4. media/ext_firm/squashfs-root/lib/libc-2.11.1.so
5. media/ext_firm/squashfs-root/lib/ld-2.11.1.so
6. media/ext_firm/squashfs-root/lib/libcrypto.so.1.0.0
7. media/ext_firm/squashfs-root/lib/libc.so.6
8. media/ext_firm/squashfs-root-0/local/sbin/snmpd
9. media/ext_firm/squashfs-root-0/local/lib/libnetsnmp.so.25.0.1
10. media/ext_firm/squashfs-root-0/local/lib/libnetsnmpmibs.so.25.0.1
11. media/ext_firm/squashfs-root-0/local/lib/libnetsnmpagent.so.25.0.1
12. media/ext_firm/squashfs-root-0/man/man8/iwpriv.8
13. media/ext_firm/squashfs-root-0/bin/webs
14. media/ext_firm/squashfs-root-0/bin/utcpdump

15. media/ext_firm/squashfs-root-0/sbin/iwlist
16. media/ext_firm/squashfs-root-0/include/wireless.h

5. Shell Scripts

If they exist then using them malicious activities are possible. The list of shell scripts are given below.

How to patch?

Privileges must be handled carefully on such file. Moreover, access should only have with the root users.

Findings

1. media/ext_firm/squashfs-root/etc/nologin.sh
2. media/ext_firm/squashfs-root/etc/bridgeoff.sh
3. media/ext_firm/squashfs-root/etc/wireless/restore.sh
4. media/ext_firm/squashfs-root/etc/wireless/reset.sh
5. media/ext_firm/squashfs-root/etc/rc.d/init.d/getIP.sh
6. media/ext_firm/squashfs-root/etc/rc.d/init.d/waitIP.sh
7. media/ext_firm/squashfs-root/etc/rc.d/init.d/start_ipconf_chk.sh
8. media/ext_firm/squashfs-root/etc/rc.d/init.d/mkprofile.sh
9. media/ext_firm/squashfs-root-0/local/sendmail.sh

6. Miscellaneous Binary Files

The extracted miscellaneous binary files are listed below:

How to patch?

They should be present in encrypted form.

Findings

1. media/ext_firm/squashfs-root/etc/wireless/regulatoryData_AG.bin
2. media/ext_firm/squashfs-root/etc/wireless/regulatoryData_G.bin
3. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/utf.bin
4. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/memtest.bin
5. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/regTest.bin
6. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/athwlan.bin
7. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/apidemo.bin
8. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/device.bin
9. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/whaltest.bin
10. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/otp_test.bin
11. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/data.rom.bin
12. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/regulatoryData_AG.bin
13. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/otp.bin
14. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/athtcmd_ram.bin
15. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/serialport.bin
16. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/perfcnt.bin
17. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/data.patch.hw2_0.bin
18. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/endpointping.bin
19. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.0/bdata.SD32.bin
20. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/utf.bin
21. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/athwlan_router.bin
22. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/fw.ram.bin
23. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/athwlan_automaton.bin
24. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/athwlan.bin
25. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/eepromw.bin
26. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/apidemo.bin

27. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/device.bin
28. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/whaltest.bin
29. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/athwlan_tablet.bin
30. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/serflash.bin
31. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/athwlan_mobile.bin
32. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/otp_test.bin
33. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/data.rom.bin
34. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/data.patch.hw3_0.bin
35. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/otp.bin
36. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/nvramconfig.bin
37. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/athtcmd_ram.bin
38. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/serialport.bin
39. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/perfcnt.bin
40. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/endpointping.bin
41. media/ext_firm/squashfs-root/etc/wireless/ath6k/AR6003/hw2.1.1/bdata.SD32.bin

7. Third Party Softwares and Libraries

FEAST has analyzed the bad release management practices followed by router firmware vendors, by the successful identification of different open source libraries and third party softwares. These libraries can be exploited thereby, causing a great security hazard. Different extracted executables like busybox, telnet, ssh, tftp, and so on are found, on which different reverse engineering techniques can be applied for injecting malicious scripts and launching the attacks.

Findings

1. media/ext_firm/squashfs-root/etc/rc.d/init.d/dropbear
2. media/ext_firm/squashfs-root/bin/telnet
3. media/ext_firm/squashfs-root/bin/tftp
4. media/ext_firm/squashfs-root/bin/busybox
5. media/ext_firm/squashfs-root/sbin/telnetd
6. media/ext_firm/squashfs-root/sbin/dropbear

8. Web Servers

The extracted web server executables are listed below:

1. media/ext_firm/squashfs-root/etc/rc.d/init.d/dropbear
2. media/ext_firm/squashfs-root/bin/login
3. media/ext_firm/squashfs-root/sbin/sulogin
4. media/ext_firm/squashfs-root/sbin/dropbear
5. media/ext_firm/squashfs-root-0/bin/webs

9. Hard Coded IP Addresses

Majority of the embedded devices use hard coded IP addresses which are used for remote code execution of malicious scripts. The monitored hard coded IP addresses are enumerated below:

1. 0.0.0.0
2. 127.0.0.0
3. 127.0.0.1
4. 131.111.255.255
5. 192.168.126.254
6. 192.168.126.255
7. 192.168.127.254
8. 192.168.127.255
9. 255.255.255.0

10. 255.255.255.255

10. Hard Coded URLs

The following are the exfiltrated hard coded URLs from the firmware binary under test:

1. http://www.hpl.hp.com

11. Email Addresses

The following are the exfiltrated hard coded email addresses from the firmware binary under test:

1. andersen@codepoet.org
2. choltje@ux1.cso.uiuc.edu.
3. c-olson@uiuc.edu
4. hare@suse.de
5. jkmaline@cc.hut.fi
6. jt@hpl.hp.com
7. rietz@mail.amps.de
8. Tim@Rikers.org

12. Hard Coded Password

Scanning of the sensitive information residing in the examined firmware binary has yeided the following hard coded passwords:

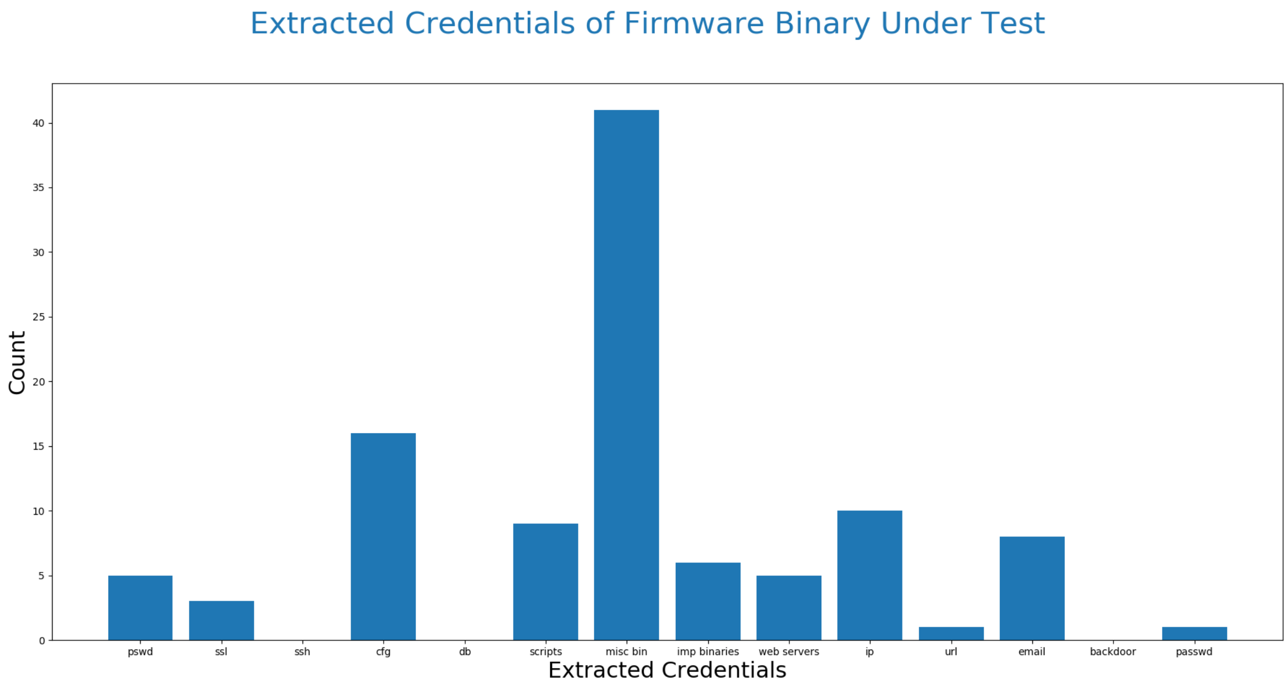
How to patch?

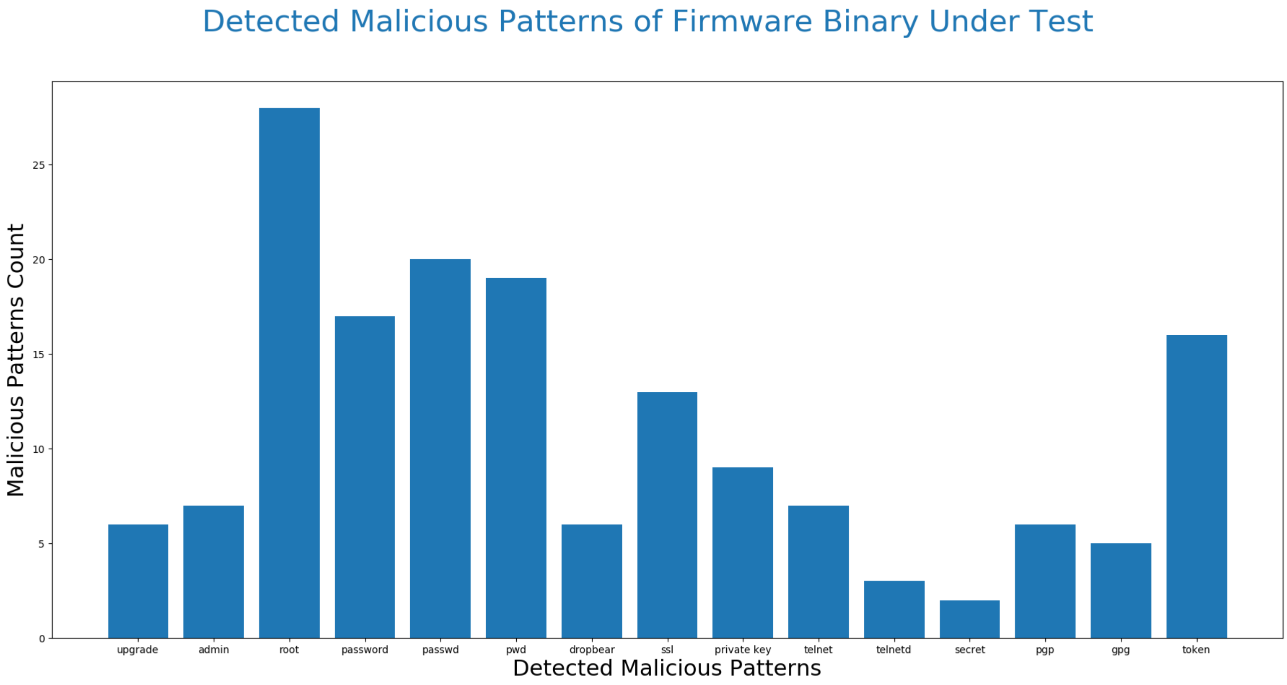
They should be present in encrypted form.

Findings

1. media/ext_firm/squashfs-root/etc/wireless/wpa_supplicant_scan.conf: password="passforsitesurvey"

Summary of Findings


Extracted Credentials of Firmware Binary Under Test
Count
pswd
ssl
ssh
cfg
db
scripts
misc bin
imp binaries
web servers
ip
url
email
backdoor
passwd
Extracted Credentials


Detected Malicious Patterns of Firmware Binary Under Test
Malicious Patterns Count
upgrade
admin
root
password
passwd
pwd
dropbear
ssl
private key
telnet
telnetd
secret
pgp
gpg
token
Detected Malicious Patterns