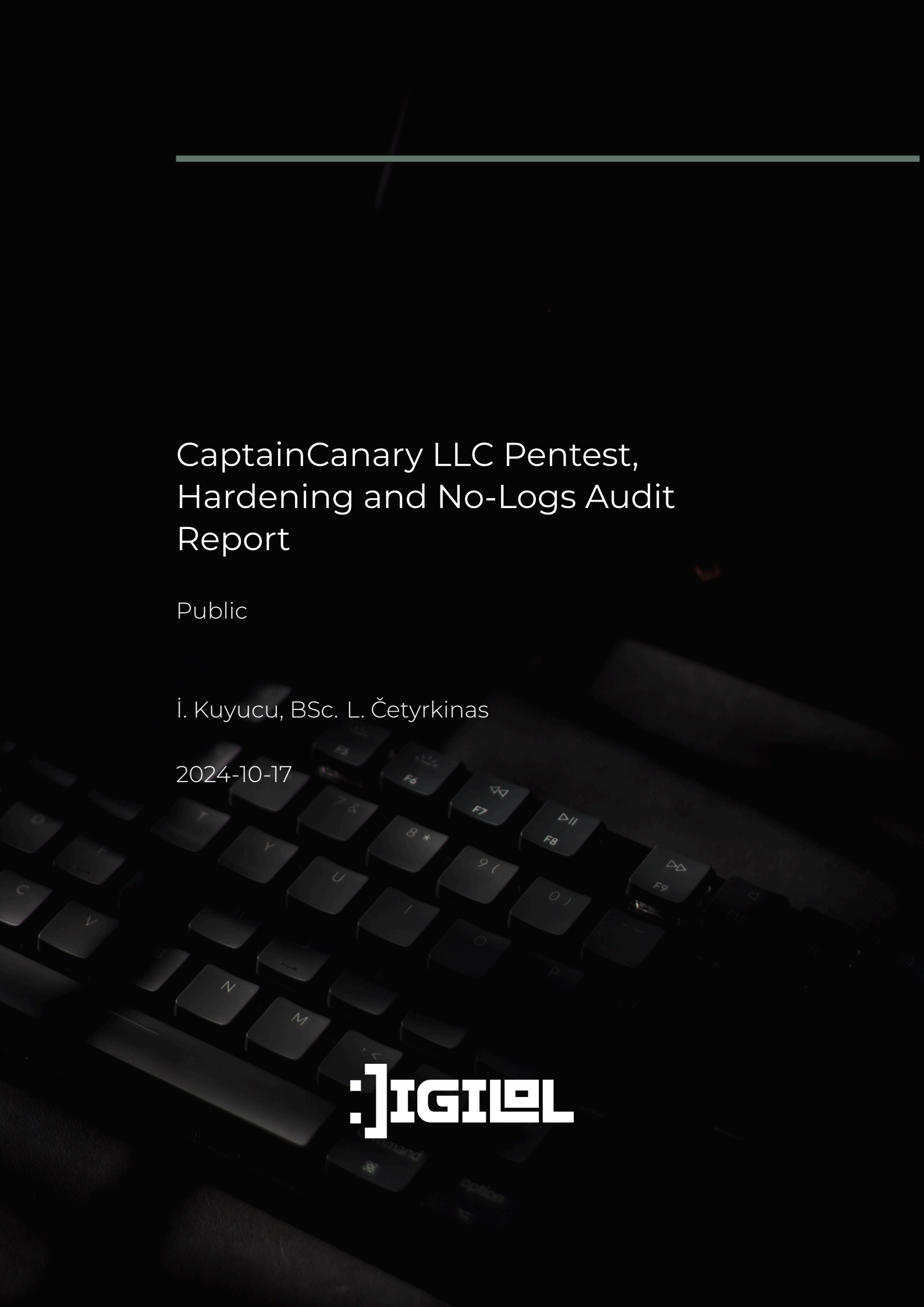
CaptainCanary LLC Pentest, Hardening and No-Logs Audit Report

Public

İ. Kuyucu, BSc. L. Četyrkinas

2024-10-17



Contents

1 Introduction 2
1.1 Executive Summary . . . 2
1.2 Findings Summary . . . 2

2 Methodology 3
2.1 Tests Performed . . . 3
2.2 Risk Assessment and Vulnerability Scoring . . . 4

3 Scope 4

4 Detailed Analysis 5
4.1 IP Spoofing . . . 5
4.1.1 Proof of Concept . . . 5
4.1.2 Recommendation . . . 7
4.2 Insecure I2P Private Key Permissions . . . 7
4.2.1 Recommendation . . . 8
4.3 unattended-upgrades Not Configured . . . 8
4.3.1 Recommended . . . 8
4.4 Insecure SimpleX Private Key Management . . . 8
4.4.1 Recommendation . . . 9
4.5 Weak Home Directory Permissions . . . 9
4.5.1 Recommendation . . . 9
4.6 GRUB Bootloader Password Not Set . . . 9
4.6.1 Recommendation . . . 9
4.7 SSH Banner Exposes OS and Version . . . 10
4.7.1 Recommendation . . . 10
4.8 Kernel Parameter Hardening . . . 10
4.8.1 Recommendation . . . 11
4.9 Missing DoS Protection in Tor Services . . . 11
4.9.1 Recommendation . . . 12

5 No-Logs Audit 12
5.1 Request IP Logging in Nginx . . . 12
5.1.1 Recommendation . . . 12

6 Version History 13

1 Introduction

This public report describes the results of the security analysis and no-logs audit conducted by Digilol OÜ on CaptainCanary LLC's infrastructre. All findings described in this report are already remediated.

CaptainCanary LLC does not log usage data of any of its services and employs measures to protect the anonymity of its users.

1.1 Executive Summary

CaptainCanary LLC engaged Digilol OÜ to conduct penetration testing against their infrastructure, and perform a security assessment to provide hardening measures.

Digilol OÜ conducted an in-depth analysis using the white-box approach and did not identify any critical vulnerabilities within the given timeframe of the assessment. However, two **medium to high severity** vulnerabilities were identified. The vulnerabilities could be exploited by an attacker to man-in-the-middle the services provided by CaptainCanary LLC or cause downtime. They are caused by insecure network configuration from the hosting provider's end and incorrect file permissions.

During the no-logs audit, Nginx within Docker was found to be logging request IP addresses.

1.2 Findings Summary

Finding	System	Severity
IP Spoofing	194.48.248.183	High
Insecure I2P Private Key Permissions	194.48.248.183	Medium
unattended-upgrades Not Configured	194.48.248.183, 185.218.124.120	Info
Insecure SimpleX Private Key Management	194.48.248.183	Info
Weak Home Directory Permissions	194.48.248.183, 185.218.124.120	Info

Finding	System	Severity
GRUB Bootloader Password Not Set	194.48.248.183, 185.218.124.120	Info
SSH Banner Exposes OS and Version	194.48.248.183, 185.218.124.120	Info
Kernel Parameter Hardening	194.48.248.183, 185.218.124.120	Info
Missing DoS Protection in Tor Services	194.48.248.183	Info

2 Methodology

The types of checks performed and how the risks were evaluated are described in this section.

2.1 Tests Performed

Network:

1. Assess the firewall.
2. Assess the network configuration of the provider.
3. Check against IP spoofing.
4. Check against ARP spoofing.
5. Check the currently open ports for exposed sensitive services.

Privilege escalation:

1. Evaluate Linux kernel and sudo versions for exploits.
2. Check Docker configuration.
3. Check Cron jobs.
4. Check Systemd services and timers.
5. Check Unix sockets.
6. Check D-Bus objects.
7. Check for SUID and SGID binaries.
8. Check for world-writable files.
9. Check for incorrect file permissions.

Services:

1. Assess Monerod deployments.
2. Assess SimpleX services.
3. Assess I2P services.
4. Assess Tor services.
5. Assess Nginx configuration.
6. Check system services (sshd, fail2ban).

Hardening:

1. Evaluate Systemd services' security.
2. Evaluate bootloader security.
3. Evaluate kernel parameters.
4. Check automated update mechanisms.
5. Check banners and identification.
6. Check system tooling (firewall, FIM, IDS/IPS).

No-logs audit:

1. Ensure sensitive information (IP, personally identifiable information) of users is not logged in existing logs.
2. Ensure there are no mechanisms present in the servers to log such information in the future.

2.2 Risk Assessment and Vulnerability Scoring

Common Vulnerability Scoring System Version (CVSS) 4.0 is used to assess the severity of the findings in this report. CVSS strings contain metrics to describe the exploitability and impact of vulnerabilities. The vulnerability severity ratings according to CVSS are low, medium, high and critical. Additionally, an informational (info) rating is included for the recommended hardening measures mentioned in this report.

3 Scope

Digilol team was authorized to perform no-logs audit and penetration testing on the following IPs and domains:

- 185.218.124.120 - Hosted on Contabo.

- 194.48.248.183 - Hosted on Cockbox.
- *.captaincanaryllc.com

4 Detailed Analysis

The findings and recommendations are explained in detail in this section.

4.1 IP Spoofing

Both IPv4 and IPv6 on the `eth0` interface are vulnerable to IP spoofing. An attacker who is a neighbor can take over the external IP addresses of CaptainCanary LLC to perform man-in-the-middle (MITM) attacks against its users or damage the reputation of the addresses by engaging in activities such as scraping, mass-scanning, or spamming.

Affected system: 194.48.248.183 (Cockbox)
Severity: High
CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:L/SI:N/SA:N/AU:Y/R:U/V:D/RE:H/U:Red

4.1.1 Proof of Concept

The initial IP addresses of the server can be observed using the `ip a l eth0` command.

```
irem@cockbox:~$ ip a l eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:16:3e:69:00:b7 brd ff:ff:ff:ff:ff:ff
    altname enX0
    inet 194.48.248.183/24 scope global dynamic eth0
       valid_lft 538sec preferred_lft 538sec
    inet6 2a00:1728:3e::c0cc:b7/128 scope global dynamic
       valid_lft 2591932sec preferred_lft 604732sec
    inet6 fe80::216:3eff:fe69:b7/64 scope link
       valid_lft forever preferred_lft forever
irem@cockbox:~$
```

Figure 1: Public IP addresses on the `eth0` interface

A malicious neighbor can discover CaptainCanary LLC's IPv4 address by checking the ARP cache or by scanning Cockbox's network ranges. Additionally it is easy to guess the IPv6 address since the IPv6 addresses on Cockbox follow a pattern and end with the last byte of the interface's MAC address.

IPv4 on the server can be changed to a neighbor's address or an unclaimed address within the range.

```
irem@cockbox:~$ sudo ip addr add 194.48.248.2/24 dev eth0
irem@cockbox:~$ sudo ip route add default via 194.48.248.1 dev eth0
irem@cockbox:~$ curl -4 ip.me
194.48.248.2
irem@cockbox:~$ sudo ip addr del 194.48.248.2/24 dev eth0
irem@cockbox:~$ sudo ip addr add 194.48.248.183/24 dev eth0
irem@cockbox:~$ sudo ip route add default via 194.48.248.1 dev eth0
irem@cockbox:~$ curl -4 ip.me
194.48.248.183
irem@cockbox:~$
```

Figure 2: Spoofing the IPv4 address

The same can be done with the IPv6 addresses.

```
irem@cockbox:~$ sudo ip addr del 2a00:1728:3e::c0cc:b7/128 dev eth0
[sudo] password for irem:
irem@cockbox:~$ sudo ip addr add 2a00:1728:3e::c0cc:b8/128 dev eth0
irem@cockbox:~$ curl -6 ip.me
2a00:1728:3e::c0cc:b8
irem@cockbox:~$ sudo ip addr add 2a00:1728:3e::2/48 dev eth0
irem@cockbox:~$ sudo ip addr del 2a00:1728:3e::c0cc:b8/128 dev eth0
irem@cockbox:~$ curl -6 ip.me
2a00:1728:3e::2
```

Figure 3: Spoofing the IPv6 address

Combining the knowledge of which services were available on the original owner of the IP address, the attacker can proceed to MITM the users.

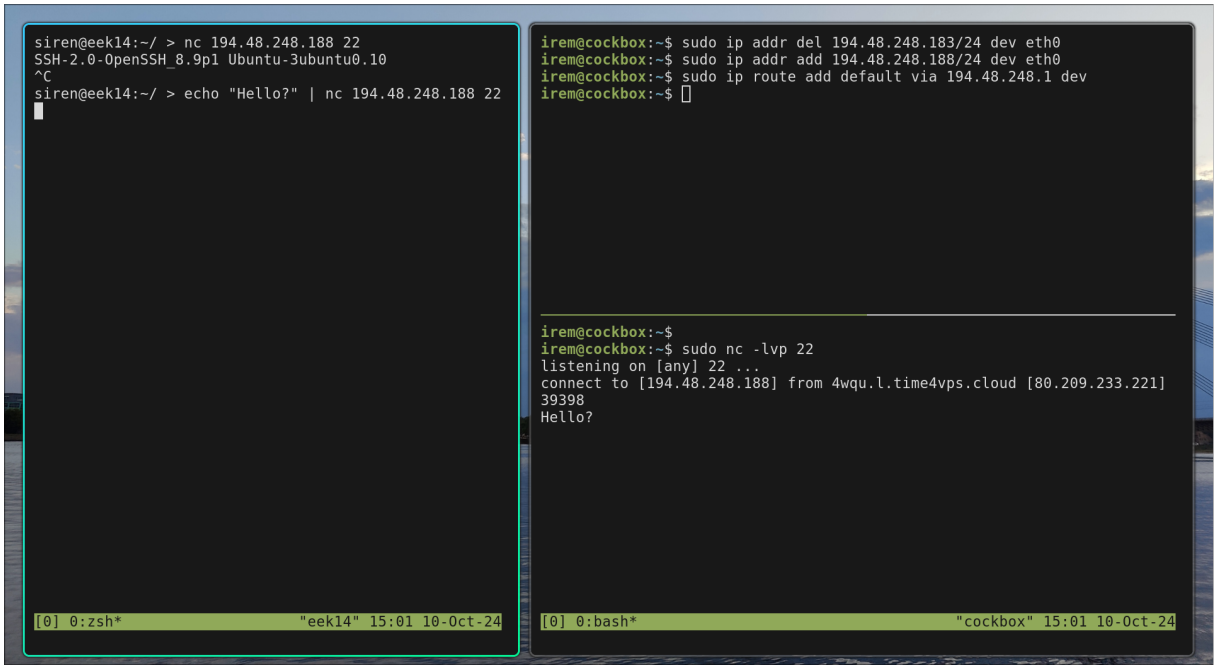


Figure 4: Man-in-the-middle proof of concept

To minimize our impact on Cockbox customers, these commands were run for only a few seconds. No credentials or sensitive information was captured during testing.

4.1.2 Recommendation

This can only be mitigated by the hosting provider since the vulnerability exists in their network configuration. Cockbox was notified of this vulnerability and a mitigation is pending.

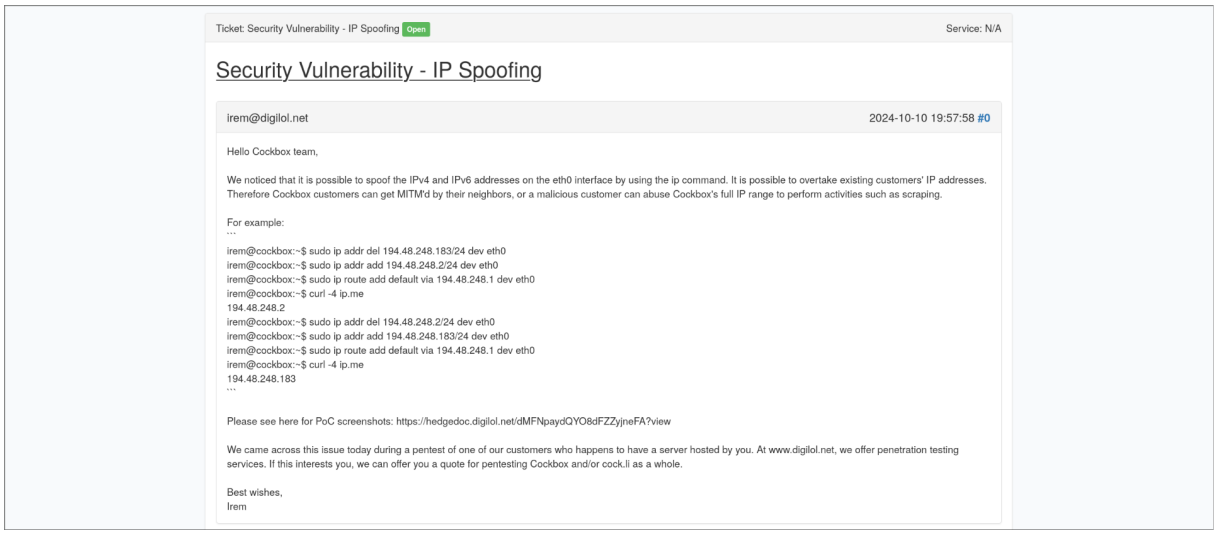


Figure 5: Opened private ticket on cockbox.org

The services hosted on this server such as SSH and SimpleX require host key verification. An attempt to MITM is not likely to capture sensitive information, unless an exception is made by the end user to proceed to connect after observing key mismatch errors. However, an attacker can still issue SSL certificates and man-in-the-middle the captaincanaryllc.com website. If this vulnerability is not mitigated in a timely manner by the hosting provider, we suggest migrating to another one.

4.2 Insecure I2P Private Key Permissions

The I2P website's private key file is world readable. An unprivileged attacker on the system can steal the keys to takeover the I2P address.

```
irem@cockbox:~$ stat /opt/docker/website-host/i2pd-data/captcanaryllc.dat
  File: /opt/docker/website-host/i2pd-data/captcanaryllc.dat
  Size: 679           Blocks: 8          IO Block: 4096   regular file
Device: 202,1   Inode: 431         Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2024-10-13 00:44:10.823841690 +0300
Modify: 2024-08-16 00:45:12.325838329 +0300
Change: 2024-08-16 00:53:39.779901244 +0300
 Birth: 2024-08-16 00:45:12.065839284 +0300
irem@cockbox:~$
```

Figure 6: File permissions of the private key `/opt/docker/website-host/i2pd-data/captcanaryllc.dat`

Affected system: 194.48.248.183 (Cockbox)
Severity: Medium
CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N/R:I/RE:L/U:Amber

4.2.1 Recommendation

Set the file permissions to 600, so only the owner can read and write to this file.

```
chmod 600 /opt/docker/website-host/i2pd-data/captcanaryllc.dat
```

4.3 unattended-upgrades Not Configured

On Debian systems, unattended-upgrades should be turned on to keep the packages up to date automatically.

Affected systems: 194.48.248.183 (Cockbox), 185.218.124.120 (Contabo)
Severity: Info

4.3.1 Recommended

Configure unattended-upgrades on the hosts by following the official Debian guide.

4.4 Insecure SimpleX Private Key Management

SimpleX SMP server's CA private key was found the server:

`/opt/docker/simplex/simplex/smp/config/ca.key`

SimpleX SMP server operators are advised to initialize their servers fully offline and to never copy the server's CA private key onto the live server. See the official server security guide for best practices.

Affected systems: 194.48.248.183 (Cockbox)
Severity: Info

4.4.1 Recommendation

Shred or delete the private key file from the server. Recreating the server with a new CA private key is also an option.

4.5 Weak Home Directory Permissions

The files in an user's home directory can be viewed by others.

Affected systems: 194.48.248.183 (Cockbox), 185.218.124.120 (Contabo)
Severity: Info

4.5.1 Recommendation

Change the home directory permissions to 750:

```
chmod 750 /home/*
```

4.6 GRUB Bootloader Password Not Set

By default anyone with physical access to the server can load alternative software or another operating system during the boot phase. Configure a password in GRUB to prevent this possibility.

Affected systems: 194.48.248.183 (Cockbox), 185.218.124.120 (Contabo)
Severity: Info

4.6.1 Recommendation

Set a password in GRUB to prevent unauthorized boot menu edits. The following script generates a random password and configures it in GRUB.

```
GRUB_PASS="$(pwgen -s 16 1)"
GRUB_PASS_HASH="$(echo -e "$GRUB_PASS\n$GRUB_PASS" | grub-mkpasswd-pbkdf2 | grep -oP
↪  'grub\.pbkdf2\.sha512\.10000\..*')"
cat <<EOF >> /etc/grub.d/40_custom
set superusers="root"
password_pbkdf2 root $GRUB_PASS_HASH
EOF
sed -i 's/class os/class os --unrestricted/' /etc/grub.d/10_linux
update-grub
echo -e "GRUB user: root\nGRUB pass: $GRUB_PASS"
```

4.7 SSH Banner Exposes OS and Version

SSH banner discloses which OS and version the host is running.

Figure 7: Banner grabbing SSH port using netcat

Affected systems: 194.48.248.183 (Cockbox), 185.218.124.120 (Contabo)
Severity: Info

4.7.1 Recommendation

Ideally, the SSH port should be firewalled to only allow specific IP addresses. Else, the information can be omitted from the banner by adding the following line to `/etc/ssh/sshd_config`:

```
DebianBanner no
```

Restart SSH service to apply the change:

```
systemctl restart ssh
```

4.8 Kernel Parameter Hardening

The following kernel parameters were found to have insecure values:

- `kernel.kptr_restrict = 0`: Kernel pointers are visible to regular users. An attacker can bypass KASLR by knowing at least one runtime kernel address.
- `net.core.bpf_jit_harden = 0`: This enables hardening for the BPF JIT compiler. Currently disabled.
- `kernel.yama.ptrace_scope = 0`: Users are allowed to use ptrace to inspect and modify running processes. This can be used to dump secrets or passwords from processes such as sshd and monerod.
- `kernel.kexec_load_disabled = 0`: Allows live-patching of the running kernel.
- `kernel.sysrq = 438`: The SysRq key can be used to run arbitrary commands that would normally require root.

Affected systems: 194.48.248.183 (Cockbox), 185.218.124.120 (Contabo)
Severity: Info

4.8.1 Recommendation

To set secure values to the above parameters, create a file `/etc/sysctl.d/90-hardening.conf` containing the following lines:

```
kernel.kptr_restrict=1
net.core.bpf_jit_harden=2
kernel.yama.ptrace_scope=2
kernel.kexec_load_disabled=1
kernel.sysrq=0
```

To apply the changes, run:

```
sysctl --system
```

The above command needs to be run only once to apply the changes for the current boot; it doesn't need to be run after every reboot.

4.9 Missing DoS Protection in Tor Services

Directives to mitigate DoS attacks over Tor network are missing from service configuration files.

Affected systems: 194.48.248.183 (Cockbox)
Severity: Info

4.9.1 Recommendation

Add the following directives to the `torrc` files where hidden services are configured:

```
HiddenServiceEnableIntroDoSDefense 1
HiddenServiceEnableIntroDoSBurstPerSec 200
HiddenServiceEnableIntroDoSRatePerSec 25
```

It may be feasible to impose stream limits with consideration to regular traffic usage and number of legitimate clients. Refer to the official Tor Project documentation for more information on DoS protection measures.

5 No-Logs Audit

One instance of Nginx serving the website https://captaincanaryllc.com was found logging access information.

5.1 Request IP Logging in Nginx

Nginx in Docker has access logs enabled.

```
website-nginx  | 85.208.96.211 - - [14/Oct/2024:18:54:11 +0000] "GET /robots.txt HTTP/1.1" 301 162 "-" "Mozilla/5.0 (compatible; Semrus
hBot/7~bl; +http://www.semrush.com/bot.html)"
website-nginx  | 85.208.96.200 - - [14/Oct/2024:18:54:11 +0000] "GET /robots.txt HTTP/1.1" 301 162 "-" "Mozilla/5.0 (compatible; Semrus
hBot/7~bl; +http://www.semrush.com/bot.html)"
website-nginx  | 185.191.171.1 - - [14/Oct/2024:18:54:12 +0000] "GET /robots.txt HTTP/1.1" 200 397 "-" "Mozilla/5.0 (compatible; Semrus
hBot/7~bl; +http://www.semrush.com/bot.html)"
canceled
root@cockbox:/opt/docker/website-host# docker compose logs -f nginx
```

Figure 8: Docker compose logs

Affected systems: 194.48.248.183 (Cockbox)
Severity: Info

5.1.1 Recommendation

Turn off `access_log` in Nginx configuration.

```
access_log off;
```

6 Version History

Document	Date
Private report release	2024-10-15
Public report release	2024-10-17