ASSURED

SECURITY CONSULTANTS

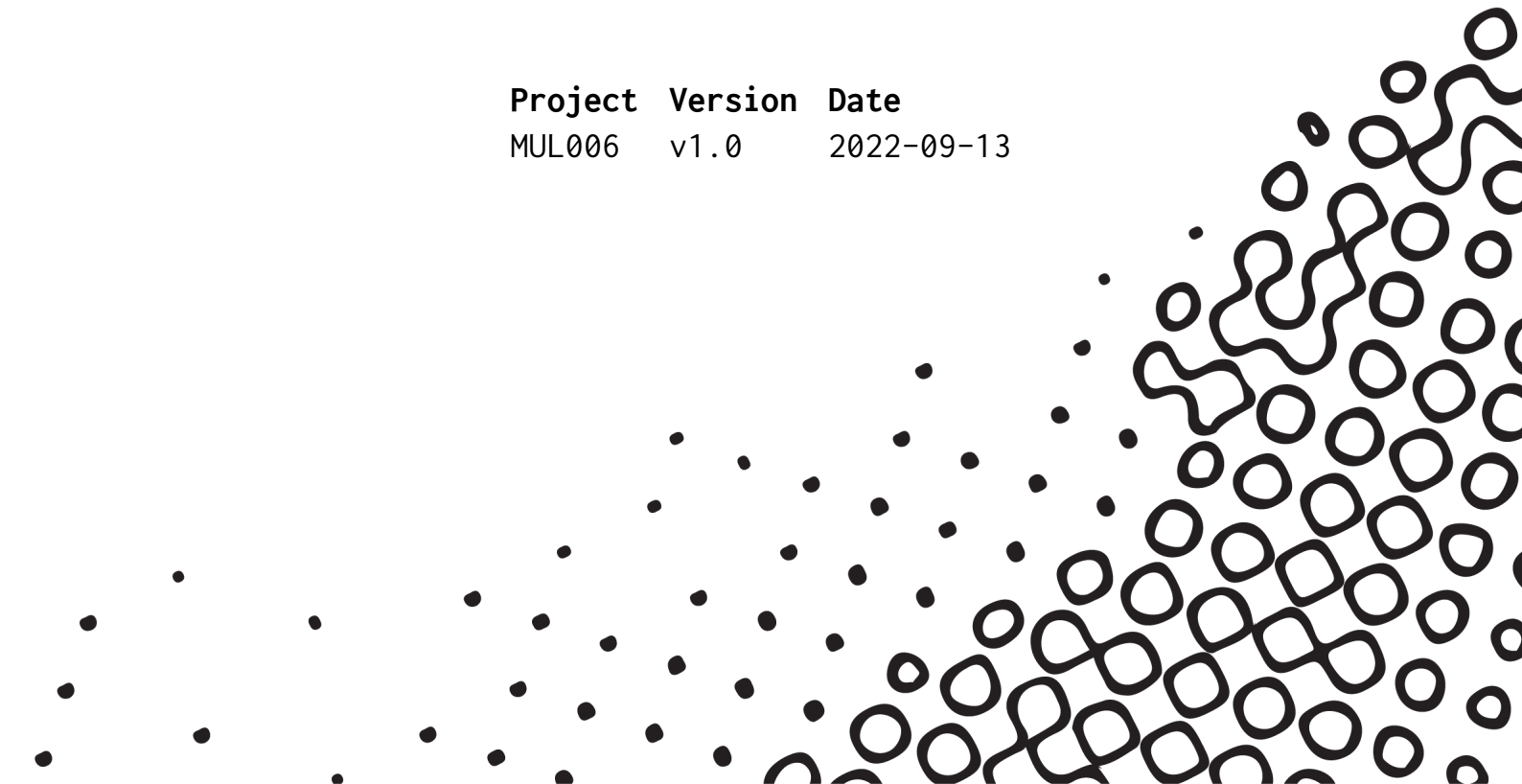
Report

CONFIDENTIAL

Mullvad DNS audit

Patrik Aldenvik, Albin Eldstål-Ahrens

Project	Version	Date
MUL006	v1.0	2022-09-13



ASSURED
SECURITY CONSULTANTS

REPORT – CONFIDENTIAL

Project	Version	Date
MUL006	v1.0	2022-05-13

Executive summary

Between 2022-04-29 and 2022-05-13 Assured Security Consultants performed a security audit on behalf of Mullvad.

Two DNS servers were in scope, one acting as an primary and one as a secondary nameserver.

This report lists the security issues found, along with recommendations for fixing or mitigating them. In our conclusions we discuss the issues and address apparent patterns in areas where security is lacking.

Several findings of category Note reflect positive practices.

Issues were found with the following risk severity assessments (number of issues):

Critical 0 | High 0 | Medium 3 | Low 7 | Note 7

The most severe findings in the report regards known vulnerabilities in installed packages, re-use of credentials between hosts and credentials written to a log file. Further improvements relate to best practices and hardening options that will enhance the overall security posture of the assessed DNS servers. The only publicly exposed service DNS is using ISC Bind. The software maintainers of ISC Bind continuously addresses vulnerabilities and releases updates, hence from an external perspective the attack surface is small. But there are hardening measures that will reduce the surface even more. Our recommendation is to calibrate the severity of the findings and address them by starting with the highest rated issues.

Assured would like to thank the Mullvad team for their support during this assessment. We are happy to answer any questions and provide further advice.

Contents

1 Introduction

1.1 Background

Assured AB (Assured) was contracted by Mullvad to perform a security assessment of their DNS servers.

1.2 Constraints and disclaimer

This report contains a summary of the findings found during the project period. This report should not be considered as a complete list of all possible vulnerabilities, security flaws and/or misconfigurations.

1.3 Project period and staffing

Assured started the project on 2022-04-29 and finished on 2022-05-13.

This report was last reviewed on 2022-09-13.

Involved in the assessment was Assured consultant Patrik Aldenvik and Albin Eldstål-Ahrens.

1.4 Risk rating

In this report we have assessed the severity of issues and identified vulnerabilities. The levels of severity are rated according to the OWASP Risk Rating Methodology [1].

Table 1: OWASP Risk Rating overall severity model

Overall risk severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

As Table 1 visualizes, the overall risk assessment is determined from a combined likelihood and impact of an identified vulnerability or security issue. A value from 0 to 9 is assessed for each variable, where 0-2 is determined LOW, 3-5 is MEDIUM and 6-9 is HIGH.

Likelihood is dependant on attributes related to threat actors and the identified vulnerability, with factors such as: the skill level and motivations

of the threat agents; how easily the vulnerability can be found and exploited, and; how likely an exploit may be detected.

Impact depends on technical and business factors, such as: level of loss of confidentiality, integrity, availability and accountability; potential financial damage; potential brand damage, and; potential violations of privacy.

Please note that the severity assessment is made by Assured consultants and ratings may differ from the resource owners' ratings.

2 Scope and methodology

2.1 Scope

2.1.1 Security assessment of DNS servers

Assured consultants were tasked with performing a security assessment of the Mullvad DNS servers. Part of this audit were two DNS servers, one acting as an primary and one as a secondary nameserver.

The main areas of interest were the following:

- Logs or information leakage that exposes the clients using the server
- Known vulnerabilities in the exposed services
- Service and system configuration should follow best security practices

For the remainder of this report, the term *customer logging* is used to mean logging of customer data, and the term *system logging* is used to refer to logging of data which is strictly unrelated to customer activity.

2.2 Methodology

2.2.1 System audit

Assured consultants were given remote administrative access to the target servers. Manual and automated analyses was performed with the aid of several tools and scripts.

The servers were running bind9 service for DNS and other services for system management and monitoring of the system health.

The vantage point of an attacker would be purely external. The scenario of assumed compromise was also investigated where analysis was performed in regards to privilege escalation from different contexts within the system.

The following system properties were audited:

- Running processes, services and scheduled jobs
- Patch level of exposed services
- Configuration of exposed services
- Firewall rule-set

- User accounts and groups
- Administrative groups and privileges
- Privileges of running services
- Hardening of kernel and running binaries
- Services and system log collection and erasure
- Common privilege escalation vectors

2.3 Limitations

The time allotted to the test was limited. The bulk of auditing was focused on networking, service and system configuration, as well as Mullvad-specific customization scripts.

3 Observations

These are the observations made during the security assessment.

3.1 Common to both DNS servers

This section outlines observations which apply to both DNS server deployments.

3.1.1 Medium Known vulnerabilities

Likelihood: MEDIUM (4), Impact: HIGH (6)

The audit indicates that the following known vulnerabilities are unpatched and the vulnerable packages are used by network exposed services. Some vulnerabilities are configuration-dependent and may not affect the servers even if the offending packages are installed.

- krb5-1.17-6ubuntu4.1: CVE-2021-37750
- openssh-server-8.2p1-4ubuntu0.4: CVE-2021-41617

CVE-2021-41617 has no fix and is dependant on the SSHd configuration options ”AuthorizedKeysCommand” and ”AuthorizedPrincipalsCommand” which are not present on the assessed server(s). CVE-2021-37750 has not been triaged. We recommend, if possible, to upgrade the packages.

3.1.2 Medium Shared SNMP credentials

Likelihood: MEDIUM (4), Impact: MEDIUM (5)

The SNMP service running on both servers have the same credentials deployed. If an attacker compromises the user credentials it will be possible to access the SNMP interfaces of all the DNS servers from the right context.

We recommend that each deployed machine receive its own unique credentials for inbound services, to enable revocation in case of a detected compromise.

3.1.3 Low Permissive firewall policy

Likelihood: LOW (2), Impact: MEDIUM (5)

The `INPUT` iptables chain (for both ipv4 and ipv6) has a default policy of `ACCEPT` and no final wildcard `DROP` rule. As a result, only specific blocking is performed.

We recommend that the default policy for `INPUT` is set to `DROP` to make sure no services are exposed by accident.

3.1.4 Low named (BIND) filesystem access

Likelihood: LOW (2), Impact: MEDIUM (4)

The NAME daemon is running with access to the root filesystem. Isolation from the root filesystem will add an extra layer of protection in the case where an attacker is able to execute code within the running BIND daemon.

We recommend running services with minimum privileges, and constrained using a chroot, jail or similar.

3.1.5 Low AppArmor profiles

Likelihood: LOW (2), Impact: MEDIUM (4)

Out of the listening network services, only `named` is confined by AppArmor.

Example 1: Services that bind sockets and are not covered by AppArmor

```
26318 /usr/sbin/snmpd not confined
28872 /usr/sbin/named confined by '/usr/sbin/named (enforce)'
32950 /usr/sbin/sshd not confined
```

Consider adding/creating profiles to restrict these services by following Ubuntus guide [2] and/or use aa-genprof to profile relevant applications during runtime.

3.1.6 Low DNS Logging

Likelihood: MEDIUM (3), Impact: LOW (2)

The BIND daemon is configured to disable all logging of DNS queries and query-related errors. In addition, the `lame-server`, `rpz`, `rate-limit` log categories are disabled.

The following log categories are enabled, with verbosity set to `debug`: `dnssec`, `resolver`, `security`, `update`, `xfer-in`, `xfer-out`, `update-security`, `delegation-only`, `config`, `general`.

No configuration is specified for the `default` category. The result of this is that BIND implicitly sends several log categories to syslog with a severity of `info`.

We recommend that a `default` category be explicitly configured, and set to discard log messages.

3.1.7 Low Kernel hardening options

Likelihood: LOW (2), Impact: MEDIUM (3)

The sysctl key `kernel.unprivileged_bpf_disabled` is set to 2 (temporarily disabled). Best practice is to set this to 1 (permanently disabled) unless BPF support is needed by unprivileged users.

The key `net.core.bpf_jit_harden` is set to 0, disabling certain BPF hardening mechanisms. We recommend setting this value to 2 (enabled for all users).

The key `kernel.kptr_restrict` is set to 1 (redact logged kernel pointers for most sources). We recommend setting this to 2 (redact logged kernel pointers from all sources).

The `CONFIG_IO_STRICT_DEVMEM` kernel option restricts the ability of `root` to access `/dev/mem` in address ranges bound to kernel drivers. With this option disabled, an attacker with `root` privileges may be able to access sensitive information which has not been logged, by inspecting the memory of the kernel.

3.1.8 Low SSHd Configuration

Likelihood: LOW (2), Impact: MEDIUM (3)

During inspection of the SSH daemon configuration it was found that:

- /etc/ssh/sshd_config is world readable
- The option ”AllowTcpForwarding” is not set and defaults to yes.
- The option ”AllowAgentForwarding” is not set and defaults to yes.
- ListenAddress is set to 0.0.0.0 but the firewall only addresses traffic on a specific interface.

We recommend to set stricter file permissions on sshd_config, address the default options ”AllowTcpForwarding” and ”AllowAgentForwarding” and also configure the ListenAddress to a specific interface.

3.1.9 Low Unnecessary installed software

Likelihood: LOW (2), Impact: MEDIUM (3)

There are some installed packages, such as tcpdump, netcat and nmap, on the server(s), which are not necessary for the functionality and also can be useful for an attacker who gets code execution on a server. There is also compilation software, such as gcc installed. For a hardened production server, it is considered best practice to remove this kind of software.

It is recommended to remove unnecessary software from the servers.

3.1.10 Note Available updates

There are installed packages which has updates that can be applied, some of the more noticeable are linux-generic* and bind9*.

Mullvad continuously makes new releases of the DNS server images and might have already updated these packages but we recommend to always keep the systems as up-to-date as possible.

3.1.11 Note Scheduled system log removal

A cron job is scheduled to run twice per week, which removes system logs `syslog`, `auth.log`, and `kern.log` and restarts the logging daemons.

Our recommendation is that this removal be performed more often, if there are no administrative reasons to maintain several days of logs.

3.1.12 Note Extraneous ModemManager service

The `ModemManager` service is running on both DNS servers, serving no apparent purpose.

We recommend disabling unused services to reduce the attack surface of the system. This recommendation also applies to non-network services such as `ModemManager`.

3.1.13 Note SSH access limited

The running OpenSSH server is protected in multiple ways:

- The firewall opens access only from specific IP addresses
- Password authentication is not permitted
- The daemon allows only specific user accounts to log in
- root login is not permitted

3.1.14 Note SSH server logs

The SSH server has verbose system logging enabled, but does not come in contact with customer data. Only administrators from pre-authorized IP addresses are allowed to attempt login via SSH.

3.2 Primary DNS server

3.2.1 Medium Password hash in logfile

Likelihood: LOW (1), Impact: HIGH (6)

The cloud-init service, used during server installation, writes sensitive information in a log file. The log file includes the username and passwordhash of the user used during installation. After installation is complete the user is removed and to read the file it requires admin privileges but if the removal step fails or the credentials are reused it poses a risk.

```
autoinstall—user—data: identity: {... password: [REDACTED] ...}
```

We recommend to disable debug logging during the installation to minimize the risk of sensitive information being written to disk and/or to remove the logfiles after a successful installation of the system.

3.2.2 Note DNS configuration

The DNS configuration is setup according to best practices, among them are:

- The DNS service is only accessible from specific IP addresses.
- TSIG, KSK, ZSK use strong cryptographic algorithms.
- DNSSEC and NSEC3 is implemented.
- Queries and Zonetransfer are only allowed from specific sources.
- NSEC3 is implemented.

3.3 Secondary DNS server

3.3.1 Note DNS configuration

The DNS configuration is setup according to best practices, among them are:

- Rate-limiting is in place.
- Recursion is only allowed from specific sources.
- The Bind version is obfuscated.

4 Conclusions and recommendations

The most severe findings in the report regards known vulnerabilities in installed packages, re-usage of credentials between hosts and credentials written to a log file.

Further improvements relates to best practices and hardening options that will enhance the overall security posture of the assessed DNS servers. The only publicly exposed service DNS is using Bind. The software maintainers of Bind continuously addresses vulnerabilities and releases updates, hence from an external perspective the attack surface is small. But there are hardening measures that will reduce the surface even more.

Our recommendation is to calibrate the severity of the findings and address them by starting with the highest rated issues.

References

[1] OWASP, “OWASP Risk Rating Methodology.” https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology, 2019.

[2] Ubuntu, “How to create an AppArmor Profile.” https://ubuntu.com/tutorials/beginning-apparmor-profile-development#1-overview.