ASSURED

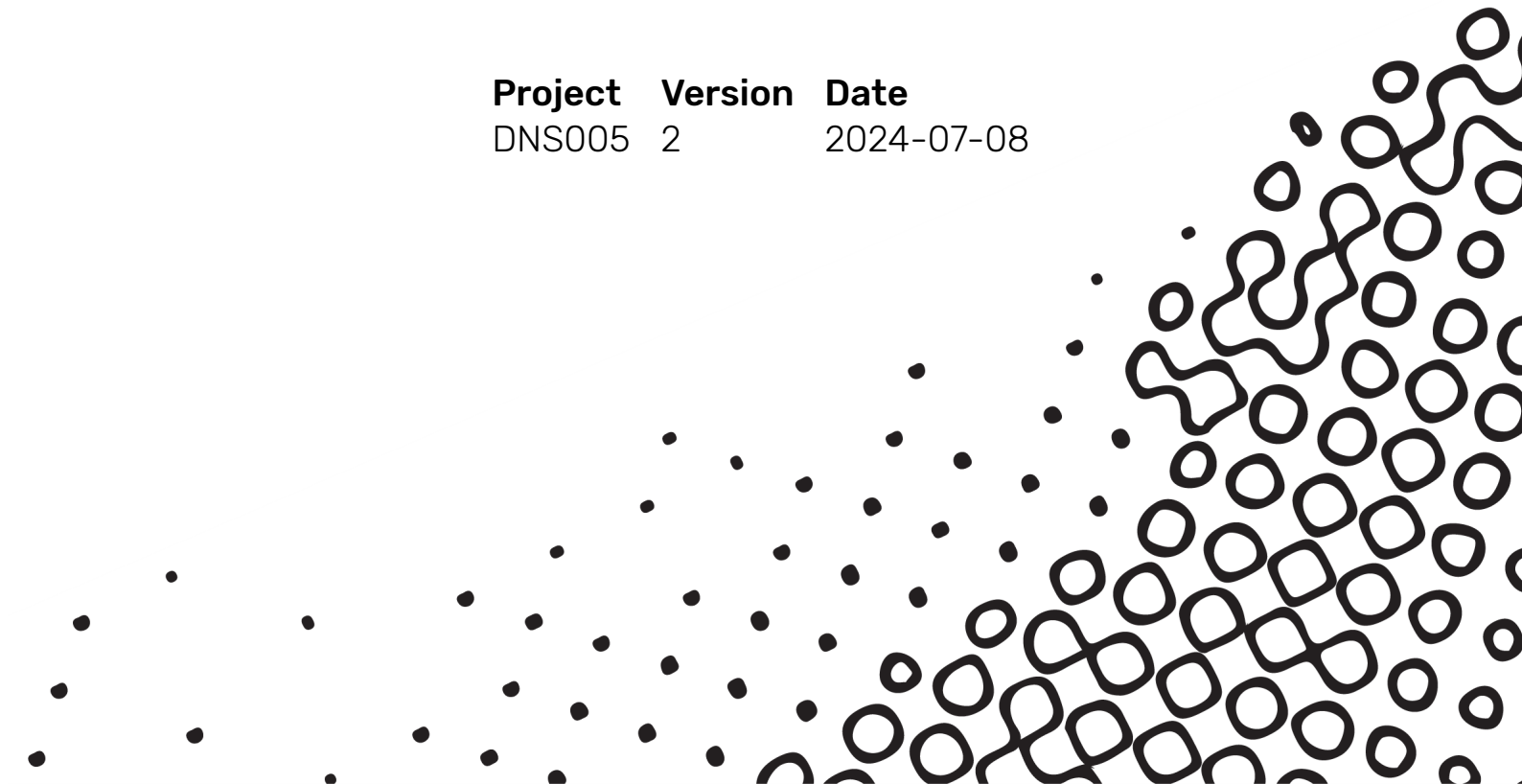
SECURITY CONSULTANTS

Report

Guardian infrastructure verification test

Patrik Aldenvik, Wictor Olsson

Project	Version	Date
DNS005	2	2024-07-08



ASSURED
SECURITY CONSULTANTS

REPORT

Project	Version	Date
DNS005	2	2024-07-08

Executive summary

Between 2024-03-18 and 2024-04-12 Assured Security Consultants performed an infrastructure audit of the Guardian app VPN infrastructure on behalf of DNSfilter.

Between 2024-06-24 and 2024-07-02, Assured was tasked with verifying the fixes and mitigations put in place as a result of the original penetration test.

The Guardian app VPN infrastructure was in scope. This included a setup of VPN relay servers and three types of backend servers responsible for serving the main application API.

The audit was executed using white-box methodology. Assured consultants were given access to code, configuration and a test setup of the infrastructure. This included the backend API servers and VPN relays.

In summary the identified issues related to network access control, service configuration, system hardening, log verbosity as well as patch/lifecycle management. No high risk issues were identified during the audit and no privilege escalation path for clients or unathenticated users was identified.

One of the primary areas of interest was to investigate logging on the VPN nodes. Guardian is keen on limiting the amount of user information on their VPN nodes to ensure user privacy. During the assessment focus was put on logging and one finding related to verbose logging was identified. That finding has been mitigated.

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

Critical 0 | High 0 | Medium 6 | Low 11

A majority of the reported vulnerabilities were fully or partially mitigated. Five observations were remaining as an accepted risk by Guardian. There is work underway to follow recommendations on four of the non fully mitigated observations.

Assured would like to thank Constantin Jacob, Will Strafach and the team at Guardian app for their support during this penetration test.

ASSURED
SECURITY CONSULTANTS

REPORT

Project	Version	Date
DNS005	2	2024-07-08

Contents

ASSURED
SECURITY CONSULTANTS

REPORT

Project	Version	Date
DNS005	2	2024-07-08

1 Observations

1.1 Server deployments

This section describes the observations made regarding the servers' configuration.

1.1.1 MED FIXED Access to backend services via Tailscale

Likelihood: LOW (2), Impact: HIGH (7)

Verification Note: Connections towards other systems via the Tailscale network from a Security gateway are now blocked.

It is possible to access systems in the backhaul Tailscale network from a Security gateway.

1.1.2 MED FIXED Permissive firewall Security gateway

Likelihood: LOW (2), Impact: HIGH (6)

Verification Note: A default DROP rule has been added to the INPUT chain.

The iptables `INPUT` chain of the Security Gateway is configured to default `ACCEPT` traffic, employing deny-listing instead of allow-listing. The Security gateway's primary function is to act as a VPN relay, forwarding traffic originating from Wireguard and IPSec tunnels served to clients. The INPUT chain however is controlling the packets destined for the host's services itself.

1.1.3 MED FIXED Outdated kernel running

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

Verification Note: The Kernel is running the latest version, automatic updates are enabled and maintenance windows are in place.

The Kernel running on several hosts has known vulnerabilities.

1.1.4 MED PARTIALLY FIXED Outdated services

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

Verification Note: Most software has been updated to the latest version. However, one piece of software requires more planning and had not been updated at the time of the verification test.

During the analysis of the running software, several of them were discovered to be outdated.

1.1.5 MED FIXED VPN node log verbosity

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

Verification Note: The reported log messages on the VPN nodes have been mitigated.

One of the primary areas of interest was to investigate logging on the VPN nodes to limit the amount of user information, to ensure user privacy.

Assured identified some verbose logging messages on the VPN nodes which could be reduced. These messages originate from the applications handling the connection of the clients.

1.1.6 MED FIXED World readable config file

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

Verification Note: The file permissions for the configuration file are now stricter.

The API config file is readable by all users on the system.

1.1.7 LOW ACCEPTED Promtail and node_exporter insecurely configured

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

Verification Note: This has been accepted as the communication is encrypted at a lower layer in the communication stack.

Promtail, that pushes logs, does not use TLS or authentication towards the central Grafana instance based on the current configuration.

1.1.8 LOW PARTIALLY FIXED Services bind to all interfaces

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

Verification Note: Some services are still listening to the wildcard interface, but access control is implemented to restrict access.

All of the hosts have multiple interfaces due to, for example, the internal administrative Tailscale network. The Security gateway is especially exposed as it has additional tunnel interfaces for handling and forwarding client traffic. All hosts in scope run services which bind their sockets to the wildcard (0.0.0.0) interface, which will make the services available on all interfaces, unless additional firewalling has been configured.

1.1.9 LOW ACCEPTED SSH internet access

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

Verification Note: SSH is the main administration interface and an alternative solution will be implemented in the future.

All hosts in scope expose the management service SSH to the Internet.

1.1.10 LOW PARTIALLY FIXED No ASLR support in application binaries

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

Verification Note: The applications developed by DNSfilter are now using ASLR.

Five of the services that are exposed externally lacks ASLR support in their binaries.

1.1.11 LOW FIXED SSHd hardening

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

Verification Note: The SSHd configuration has been hardened.

SSH is enabled on all of the servers for administrative access. Hardening and limiting services which are used for administrative access is a common best practice and highly encouraged.

1.1.12 LOW ACCEPTED Strongswan configuration

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

Verification Note: The Strongswan configuration supports the insecure Diffie-Hellman group modp1024. That group is the most secure option which Windows 7 through 11 supports by default.

During analysis of the Strongswan configuration on the security gateway, it was found that a connection proposal is using an insecure Diffie-Hellman group.

The `ikev2_windows10` connection in the Strongswan configuration (swanctl.conf) proposes an insecure Diffie-Hellman group, `modp1024`. This group uses a 1024 bit prime number and has been deemed broken[1]. Although further research shows that this is required to support Windows default configuration[2].

[1] `https://wiki.strongswan.org/projects/strongswan/wiki/SecurityRecommendations/50#Broken-Algorithms`

[2] `https://docs.strongswan.org/docs/5.9/interop/windowsClients.html#strong_ke`

1.1.13 LOW ACCEPTED Unauthenticated Redis

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

Verification Note: The service is still unauthenticated and it is accepted for now. But there is work in progress to mitigate this.

Redis is running without authentication on the loopback interface on the Security gateway. If an attacker gains a low privilege foothold on the server, this could be abused to interact with the privileged service which controls configuration of IPsec and Wireguard tunnels.

1.1.14 LOW FIXED Haproxy does not validate TLS

Likelihood: LOW (1), Impact: MEDIUM (4)

Verification Note: The identity of the destination server is now verified to be signed by trusted certificate authorities.

Haproxy is used for load balancing of the backend API. When reviewing its configuration, we identified that TLS validation was disabled towards an internal API server.

1.1.15 LOW FIXED Postgres database hardening

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

Verification Note: The PostgreSQL configuration is hardened.

Three PostgreSQL parameter settings for the database could be improved. Many databases often come configured with insecure defaults which can be improved to strengthen the security posture of the application and the data it houses.

1.1.16 LOW FIXED AppArmor profiles lacking on exposed services

Likelihood: LOW (1), Impact: MEDIUM (3)

Verification Note: Sandboxing is implemented using an alternative to AppArmor.

Part of the audit was to investigate use of sandboxing. AppArmor is common to use to restrict an applications ability to interact with only the bare minimum system functionality required for its operation. Configuring and using such profiles is recommended for exposed applications to limit available functionality to an attacker in the event of exploitation.

1.2 GCP environment

This section describes the observations made regarding the cloud instance.

1.2.1 LOW ACCEPTED Default service account

Likelihood: MEDIUM (3), Impact: LOW (1)

Verification Note: The VMs running in GCP is using the default service account but the permissions are not abuseable in the current environment. Work is under way to find a more permanent solution.

The hosts in GCP are using the default service account. The default Compute Engine service account has the Editor role on the project which allows read and write access to most Google Cloud Services. It should be noted that even though the privileges assigned to this service account are equivalent to the Editor role, it is restricted from accessing some services via Access scopes[3].

[3] https://cloud.google.com/compute/docs/access/service-accounts#default_scopes