Pentest-Report NordVPN VPN Servers & Infra. 10.2025

Cure53, Dr.-Ing. M. Heiderich, D. Mao, Y. Chun Chu, M. Piechota, Y. Yuan

Index

Introduction

> *"We strive to make the internet better than it is today. It can be free from online threats, censorship, and surveillance, as envisioned in 1989 — the year the World Wide Web was invented."*

From https://nordvpn.com/about-us/

This report describes the results of a penetration test and security assessment of the NordVPN VPN servers and infrastructure. Implemented as a gray-box inspection and tracked as *NOR-28,* this project was completed by Cure53 in October 2025.

To offer some contextual details about the broader cooperation and project-specific resources, it should be noted that the work was requested by UAB 360 IT in September 2025. The investigation was planned as part of the long-standing cooperation between Cure53 and UAB 360 IT/ NordVPN teams.

While over twenty projects were commissioned to Cure53 in the frames of joint security efforts, the security of the NordVPN servers and infrastructure was, in particular, assessed during several prior engagements, including *NOR-17* in June 2024 and *NV-03* in September 2022.

As far as *NOR-28* is concerned, the Cure53 testing team examined the scope in late October 2025, namely in CW43, with a total of twenty-one days invested to reach the coverage expected for this project. A team consisting of five senior testers was formed and assigned to the preparation, execution, documentation, and delivery of this project.

Given the scope, the work was contained in a single work package (WP):

- **WP1:** Tests, audits & assessments of NordVPN VPN servers and infrastructure

The gray-box methodology was chosen for this project. A list of areas in focus and Teleport access were provided to Cure53. All further means of access required to complete the tests were guaranteed as well.

All preparations were done in mid-October 2025, namely during CW42, so as to ensure a smooth transition into the testing stage for the Cure53 team. Communications during the test were done using a dedicated shared Slack channel between the teams of UAB 360 IT and Cure53. All involved personnel from both parties could join the discussions on Slack.

Cure53 did not need to ask many questions, and the quality of all project-related interactions was consistently excellent. Although the testers offered frequent status updates on the examination and emerging findings, live-reporting was not used during this project. Continuous communication contributed positively to the overall results of this project. Significant roadblocks were avoided thanks to clear and careful preparation of the scope, as well as through subsequent support.

The Cure53 team managed to acquire good coverage of the WP1 targets. Of the nine findings spotted during this *NOR-28* inspection, five were classified as security vulnerabilities. This indicates that the remaining four tickets contain general weaknesses with lower exploitation potential.

The VPN servers managed by NordVPN were generally found to be well-hardened. They were observed to utilize a robust container isolation strategy to segregate services. A restrictive network posture, enforced by *nftables*, was also confirmed by the assessment's team.

The layered defense-in-depth approach taken by NordVPN was positively evaluated. Specifically, it was clearly apt in successfully preventing unauthorized access attempts against critical components like the *nordproxy* solution. At the same time, given its crucial role for the ecosystem, a full source code review of the components is recommended.

Despite various hardening mechanisms in place, several *High*-impact vulnerabilities related to local privilege boundaries were identified. Two distinct privilege escalation paths to *root* were discovered via misconfigurations in *sudo* (NOR-28-002) and Docker group memberships (NOR-28-003), respectively.

Furthermore, Cure53 discovered issues concerning overprivileged or non-expiring tokens. These affected various components, including *Consul* (NOR-28-008) and *Teleport* (NOR-28-001). Drawing on these results, Cure53 would argue that local access control configurations grant broader permissions than necessary. As such, they require a dedicated review to ensure adherence to the principle of least privilege.

The following sections first describe the scope and key test parameters, the material available for testing, as well as how the work package was structured and organized.

Next, all findings are discussed in grouped vulnerability and miscellaneous categories. The problems are then discussed chronologically within each category. In addition to technical descriptions, PoC and mitigation advice is provided where applicable.

The report ends with general conclusions relevant to this autumn 2025 project. Based on the test team's observations and the evidence collected, Cure53 elaborates on the overall impressions and reiterates the verdict. The final section also includes tailored hardening recommendations for the NordVPN VPN servers and infrastructure.

Identified Vulnerabilities

The following section lists all vulnerabilities and implementation issues identified during the testing period. Notably, findings are cited in chronological order rather than by degree of impact, with the severity rank offered in brackets following the title heading for each vulnerability. Every finding has been given a unique identifier (e.g., *NOR-28-001)* to facilitate any follow-up correspondence in the future, if required.

NOR-28-001 WP1: *Teleport invite* tokens do not expire after use *(Low)*

***Fix Note**: This issue has been fixed by the development team and verified by Cure53 to be working as expected. The described issue no longer exists.*

NordVPN uses *Teleport* to SSH into its VPN servers. To register new nodes on the main *Teleport* server, an *invite* token is required to authenticate the new node. Each node stores an *invite* token on disk, which is used to authenticate to the *Teleport* server when first registering itself. Notably, this token never expires and is shared across all NordVPN nodes.

As a result, if any of these components are compromised, the token can be used by an attacker to create an unlimited number of *Teleport* nodes in the cluster. An attacker could use this to create a fake node with a similar name to a real node, and MitM keystrokes when a NordVPN staff member accesses the node via *Teleport.*

NOR-28-002 WP1: Privilege escalation with *nagios* user via *sudo* abuse *(High)*

***Fix Note**: This issue has been fixed by the development team and verified by Cure53 to be working as expected. The described issue no longer exists.*

Whilst analyzing the NordVPN server's *sudo* configuration, it was determined that the *nagios* user can execute any binary under */usr/lib/nagios/plugins/* as *root* without a password. Since several plugins either execute arbitrary commands (e.g., *urlize*, *remove_perfdata*, *negate*) or accept options enabling code execution without dropping privileges (e.g., *check_by_ssh*), this permits a direct local privilege escalation from *nagios* to *root*.

NOR-28-003 WP1: *Telegraf* user privilege escalation via Docker *(High)*

***Fix Note**: This issue has been fixed by the development team and verified by Cure53 to be working as expected. The described issue no longer exists.*

During a review of the NordVPN server's user group configurations, it was found that the *telegraf* user is a member of the *docker* group, allowing them to use Docker even without having *root* privileges.

NOR-28-006 WP1: Unresolved issue from previous test *(Low)*

***Client Note**: The potential risk associated with this issue has been formally accepted by the client. Based on their assessment, the decision has been made to omit the fix, acknowledging the residual risk.*

During this assessment, it was observed that a previously reported finding regarding unrestricted outbound firewall connections remains unresolved. This configuration continues to permit systems within the network to initiate connections to any external destination without limitation.

As noted in the report linked to the prior engagement and tracked as *NOR-17-008*, such permissive egress filtering presents a security risk. It possibly translates to enabling compromised systems to establish communication with external command and control servers, exfiltrate data, or stage further attacks.

NOR-28-008 WP1: Catalog poisoning via over privileged token *(Medium)*

***Fix Note**: This issue has been fixed by the development team and verified by Cure53 to be working as expected. The described issue no longer exists.*

While accessing the NordVPN staging infrastructure, a *Consul* client token embedded within a container at */etc/consul.d/consul.hcl* was found to possess excessive privileges. The token, configured with ACL policy *agent-token*, includes global *node:write* permissions. Resultantly, it enables arbitrary *Catalog* node creation, modification, and deregistration across both *eu* and *eu-aws* regions, without requiring *gossip ring* membership.

The vulnerability was demonstrated by registering fake nodes (*cu5301*, *cu5302*) and temporarily overwriting an existing node (*nl1040*) through the *Catalog* API. Through the reproduction steps, it can be seen that the downstream *FreeRADIUS* templates automatically generated configuration entries for the injected node names.

While firewalls and database validations are sourced independently from the *Catalog* components, the primary implications could entail configuration churn and potential Denial-of-Service (DoS) problems caused by node deregistration or malformed entries.

Miscellaneous Issues

This section covers any and all noteworthy findings that did not incur an exploit but may assist an attacker in successfully achieving malicious objectives in the future. Most of these results are vulnerable code snippets that did not provide an easy method by which to be called. Conclusively, while a vulnerability is present, an exploit may not always be possible.

NOR-28-004 WP1: Overly permissive *log shipper* role *(Low)*

***Fix Note**: This issue has been fixed by the development team and verified by Cure53 to be working as expected. The described issue no longer exists.*

During the assessment, credentials for the *log shipping* user *fluent* were discovered. Although the target ELK host was unreachable from the tested system, the associated role permissions were verified with the responsible team. Ultimately, this review revealed excessive privileges beyond those needed for *log shipping.*

Cure53 confirmed that the holder of this role could read, update, and delete permissions across numerous indices, along with possessing modification rights for index templates. Compromise of these credentials could make it possible for an attacker to read logs, tamper with or delete log evidence, and more generally disrupt log processing.

NOR-28-005 WP1: *VictoriaMetrics* configured to ignore SSL errors *(Info)*

***Fix Note**: This issue has been fixed by the development team and verified by Cure53 to be working as expected. The described issue no longer exists.*

NordVPN uses *vmagent* of *VictoriaMetrics* to push limited metrics data to a centralized collector. Currently, *vmagent* is configured to ignore SSL verification errors, making it possible for an advanced attacker to gain traction.

Specifically, an adversary who can intercept traffic between the VPN node and metrics collection service could intercept and modify metrics data. In certain scenarios, this could potentially impact the integrity of the collected metrics.

NOR-28-007 OOS: NordWhisper client does not pin CA certificate *(Low)*

While testing the NordWhisper server, it was found that the Linux NordVPN client does not pin the CA certificate for NordWhisper connections. A sophisticated attacker able to issue a TLS certificate for a NordVPN node could intercept all NordWhisper traffic, as long as they are operating in the network path between the victim and NordVPN server.

Cure53 recommends only trusting specific NordVPN issued CA certificates for NordWhisper connections.

NOR-28-009 WP1: SSH demon allows *root* login *(Info)*

***Client Note**: The potential risk associated with this issue has been formally accepted by the client. Based on their assessment, the decision has been made to omit the fix, acknowledging the residual risk.*

During a review of the NordVPN server's *sshd* configuration, it was found that the *PermitRootLogin* option is set to *yes*, which makes it possible to connect to the server as the *root* user. It is generally recommended to disallow this, as it means attackers do not have to guess a username to connect. Fortunately, password authentication is correctly disallowed, rendering this mode of attack impossible.

Still, requiring authentication as a different user before performing privileged actions can help improve accountability and add an extra layer of security.

Conclusions

This *NOR-28* assessment covered host-level hardening, core service configurations, and the VPN authentication stack. Performed by five members of the Cure53 team in a gray-box manner, the project revealed the presence of nine security-relevant problems negatively impacting the scope of the NordVPN VPN servers and infrastructure. While no issues with *Critical*-scored risks could be spotted, two items received *High*-impact markers, thus calling for urgent remediation.

As for some detailed observations, this October 2025 review of the host's network posture confirmed some positive indicators related to security, for example in the form of restrictive *nftables* ruleset. Locally running services, including *Nagios,* were investigated for command injection vectors but found to be properly secured.

In-depth analysis of how NordVPN uses *Teleport* to manage its servers was performed. In this area, it was noted that the *authentication* token used to instantiate new servers on the *Teleport* authentication server does not expire and is reused across all NordVPN nodes (NOR-28-001).

A significant deep-dive was performed on the *FreeRADIUS* and *OpenVPN/strongSwan* authentication logic. The EAP handling mechanism was specifically investigated for a potential authentication bypass, but it was concluded that the configuration is set in accordance with standard practices. No vulnerabilities could be spotted.

Next, a detailed static and dynamic analysis was performed on the custom *nordproxy* solution, which was noted to be a migration from the previously used *Squid* component. Numerous attempts were made to bypass the new component’s denylist logic, with the hopes of gaining access to local administrative services.

Despite multiple techniques employed by the testers, these attempts were unsuccessful. While this is a positive outcome, the critical role of this component should not be disregarded. As such, a full source code review of this solution is highly recommended.

During examination of user group memberships, the *telegraf* user account was found to be a member of the *docker* group (NOR-28-003), enabling Docker access without *root* privileges. This configuration permits immediate privilege escalation to *root* by mounting the host filesystem in a container, thereby bypassing other access controls.

Along with the *nagios* privilege escalation issues (NOR-28-002), these findings demonstrate that local privilege boundaries require more attention. To prevent undermining the defenses provided by container isolation, hardening needs to be done before this becomes a systemic issue for NordVPN.

The outcomes of the SSH configuration review must highlight that *root login* is permitted (NOR-28-009). While this does not represent an immediate security risk due to proper disabling of password authentication, restricting *root login* is still considered a more optimal solution, given that it can provide some additional security.

A review of the configurations of various services running in Docker containers was conducted and no deviations from best practices were identified. A notable exception to this is that logging was found to be broadly disabled across the inspected services. However, in the context of preserving user privacy, this is an appropriate configuration.

Some plaintext credentials for external services like RADIUS and Kafka were identified in configuration files. However, these files were not accessible to unprivileged users.

During assessment of the *Consul* configuration within the containerized infrastructure, excessive privileges were found in the *agent* token located in */etc/consul.d/consul.hcl* (NOR-28-008). The token possesses global *node:write* permissions across all regions, enabling node registration, modification, and deregistration through the *Catalog* API.

Testing demonstrated successful injection of fake nodes and temporary overwriting of existing nodes. While downstream security controls - such as firewalls and database validations - operate independently from the *Catalog,* this vulnerability enables configuration churn and service disruption through node manipulation.

Subsequent analysis of *sudo* configurations demonstrated that a privilege escalation path exists in the *nagios* user account (NOR-28-002). The *sudo* rule grants passwordless execution of any binary under */usr/lib/nagios/plugins/*, which includes plugins that execute arbitrary commands or accept options facilitating code execution. This configuration provides a direct escalation path from *nagios* to *root* privilege-levels.

On the whole, the findings demonstrate access control configurations that grant broader permissions than necessary for operational requirements. It is recommended to conduct a systematic review of privilege assignments across infrastructure components to ensure adherence to the principle of least privilege, particularly for tokens, service accounts, and *sudo* configurations that enable elevated access.

Contrarily, a comprehensive review of file permissions on the server concluded with no findings to report. Positively, all sensitive files were only accessible for the *root* user, while non-*root* users had no way of editing configuration files.

Moving on to the review of the *VictoriaMetrics* telemetry client, Cure53 noted that this component does not have SSL certificate validation enabled (NOR-28-004). As a consequence, an attacker on the network path between the NordVPN node and the telemetry server could intercept and potentially modify telemetry data. This problem negatively affects the integrity of the data reported.

In parallel to the core review, an out-of-scope finding was noted on the Linux NordWhisper client (NOR-28-007), which trusts system CA certificates instead of pinning a NordVPN-specific certificate. Combined with an unresolved finding from a previous pentest (*NOR-17-007*), this would be beneficial for an attacker who has compromised any single NordVPN node. Leveraging this chain of issues, they could decrypt traffic to all NordVPN nodes, as long as the attacker is in the network path of the victim.

Finally, the container hardening strategy was examined and found to be robust, as evidenced by services running with appropriately limited capabilities. During this review, however, credentials for the fluent log shipping user were discovered (NOR-28-004). Although the target ELK host was unreachable from the tested system, a subsequent review of the associated role confirmed that it possesses excessive privileges that need to be adjusted.

Overall, NordVPN’s VPN servers have already been properly hardened. Most importantly, each service appears to be isolated to its own Docker container to help prevent lateral movement if a single service is compromised. However, more care should be taken to ensure that if the entire server is compromised, an attacker cannot affect NordVPN clients connecting to other servers.

Cure53 recommends ensuring that all secrets are unique between different NordVPN nodes, so that a compromise of one server can have a more local impact. For instance, it would be optimal to have a way to revoke specific secrets without affecting the rest of the network.

Last but not least, many of the services inspected during *NOR-28* are running first-party binaries which make them difficult to test thoroughly. Cure53 recommends a more in-depth source code review of these services.

Cure53 would like to thank Laurynas Jankevičius, Kasparas Bražėnas and Evaldas Vasiliauskas from the UAB 360 IT team for their excellent project coordination, support and assistance, both before and during this assignment.