



Zenlayer, Inc.

External Network Penetration Testing Report

v 1.4

| March 5, 2026



Copyright

© Copyright Discloze, Inc., 2026. All Rights Reserved. This is unpublished material and contains trade secrets and other confidential information and is subject to a confidentiality agreement. The unauthorized possession, use, reproduction, distribution, display, or disclosure of this material or the information contained herein is prohibited.

The methodology used to test the computer systems is considered proprietary intellectual information of Discloze and may not be disclosed without written permission from Discloze. Discloze gives permission to copy this report for the purposes of disseminating information within your organization or to any regulatory agency.

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such, it should be afforded the security and handling precautions that a confidential document warrants. Controlled distribution to relevant parties only is advised, and copying without written permission is prohibited.

Discloze treats the contents of a security assessment as company confidential material and will not disclose the contents of this document to anyone without written permission. Confidential information in this report is intended only for Zenlayer, Inc. and is bound by a non-disclosure agreement. All unauthorized use or disclosure is strictly prohibited.

Table of Contents

Executive Summary	4
Scope.....	4
Engagement Timeline.....	4
Methodology	4
External Network	4
Severity Distribution Across Risk Categories (6)	6
Risk Accepted (6).....	7
Technical Details.....	8
Engagement Timeline and Testing Objectives	8
Scope.....	8
Attack Narrative	8
External Network Assessment	9
Appendix A: Methodology	11
Testing Standard.....	11
Applicable Standards and Guidance	11
Summary of Methodology	11
Appendix B: Risk Rating	12
Quantitative Rating	12
Qualitative Rating	13
Risk Assessment Guidelines.....	14
Appendix C: References.....	16
Document Tracking	19
Contact Information.....	19



Executive Summary

Scope

Discloze recently conducted an unauthenticated external network penetration test on behalf of Zenlayer, Inc. ("Company") to evaluate the security posture of Zenlayer's internet-facing infrastructure and exposed services. The primary objective was to identify security weaknesses observable from the public internet and provide actionable recommendations to mitigate the risks associated with these findings.

In Scope
• Wildcard Domains: ○ *.zenlayer.com ○ *.zenlayer.cn ○ *.zenlayer.net ○ *.zenlayer.win ○ *.zenlayer.ai ○ *.zenlayer.in ○ *.zenlink.net ○ *.zenlogic.net ○ *.zenworks.net ○ *.theturbo.ai ○ Other related IPs

Engagement Timeline

December 2025

Methodology

Discloze employed a comprehensive testing methodology focusing on the OWASP Top 10 and external network security, encompassing multiple stages designed to simulate real-world cyber threats.

External Network

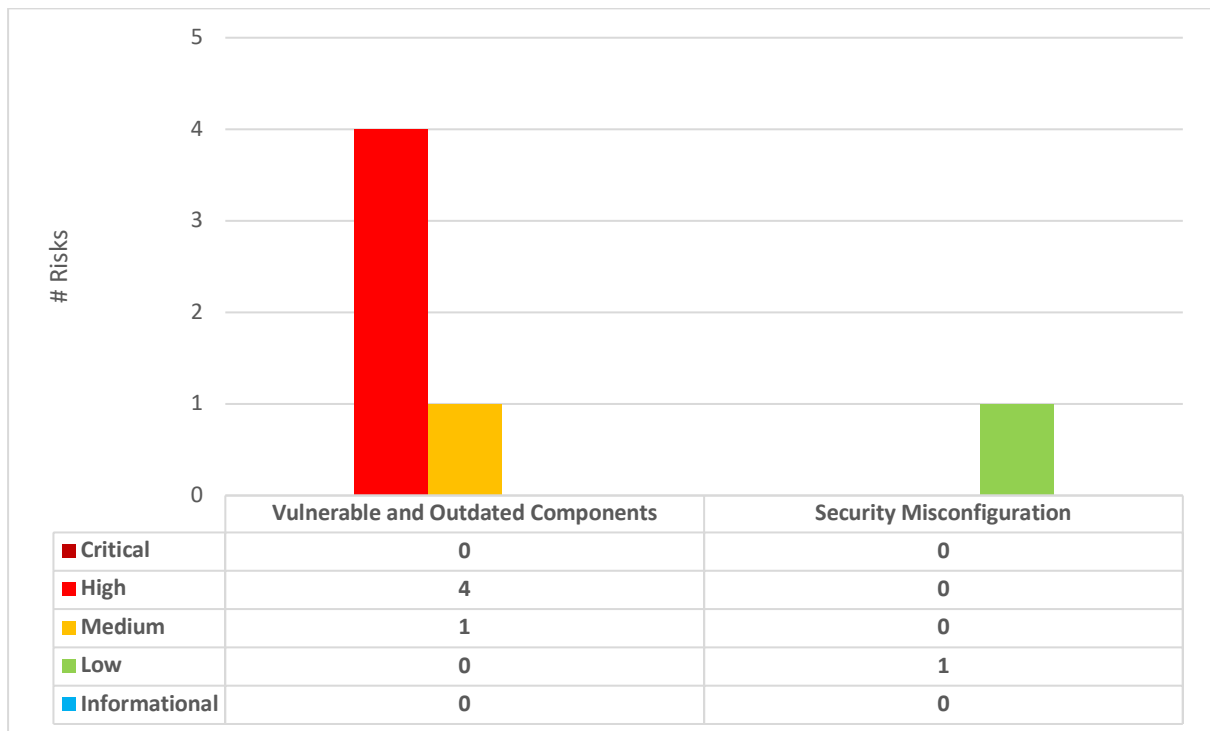
- **Reconnaissance:** Gathering information about the target network, including active IPs, open ports, and exposed services, to identify potential attack vectors.
- **Vulnerability Scanning:** Automated scanning to identify known vulnerabilities (including CVEs) in exposed services and systems.



- **Subdomain and DNS Testing:** Identifying subdomains and testing for misconfigurations, including subdomain takeover vulnerabilities.
- **Exploitation:** Actively attempting to exploit identified vulnerabilities (e.g., weak authentication, protocol exploits) to assess their impact.
- **Post-Exploitation Analysis:** Evaluating the extent of access, pivoting opportunities, and potential damage from successful exploits.

These procedures were meticulously designed to evaluate the organization's security defenses against various attack vectors.

Severity Distribution Across Risk Categories (6)



Risk Accepted (6)

ID	Severity	Category	Risk
H – 1	High	Vulnerable and Outdated Components	Outdated Nginx Instance on smartmonitor.zenlayer.win Leading to Multiple CVEs - 6 CVEs
H – 2	High	Vulnerable and Outdated Components	Outdated Nginx Instance on points.zenlayer.net Leading to Multiple CVEs - 5 CVEs
H – 3	High	Vulnerable and Outdated Components	Outdated Nginx Instance on zga-api.ecn.zenlayer.net Leading to Multiple CVEs - 6 CVEs
H – 4	High	Vulnerable and Outdated Components	Outdated Nginx Instance on traffic.zenlayer.com.c.zenlayer.net Leading to Multiple CVEs - 5 CVEs
M – 1	Medium	Vulnerable and Outdated Components	Outdated NGINX 1.27.5 on ce.zenlayer.net Exposing CVE-2025-5385
L – 1	Low	Security Misconfiguration	Expired SSL Certificates on ipt-hkg-k8s-external.zenlink.net and zrt-sgp-k8s-external.zenlink.net

Technical Details

Engagement Timeline and Testing Objectives

Discloze conducted a comprehensive external network penetration test of Zenlayer's internet-facing infrastructure to identify vulnerabilities that could be exploited by an unauthenticated or external attacker. The assessment focused on network-layer and perimeter-exposed services, including publicly reachable hosts, open ports, service configurations, encryption/TLS posture, and common external attack paths such as misconfigurations and weaknesses in exposed protocols or administrative interfaces.

The findings and recommendations in this report are intended to help Zenlayer reduce external attack surface, remediate perimeter weaknesses, and strengthen the confidentiality, integrity, and availability of systems accessible from the public internet. This engagement reflects Zenlayer's and Discloze's shared commitment to continuous security improvement and resilient external-facing operations.

Scope

The testing commenced on December, 2025

The following wildcard domains were in scope:

- *.zenlayer.com
- *.zenlayer.cn
- *.zenlayer.net
- *.zenlayer.win
- *.zenlayer.ai
- *.zenlayer.in
- *.zenlink.net
- *.zenlogic.net
- *.zenworks.net
- *.theturbo.ai
- Other related IPs

Attack Narrative

The objective of the external network penetration test was to identify and validate vulnerabilities in Zenlayer's internet-facing systems and exposed services that could be leveraged by an external attacker to gain unauthorized access, disrupt availability, or enable data exposure. Where feasible, Discloze attempted controlled exploitation to



confirm real-world impact and then provided actionable remediation recommendations to reduce risk and strengthen Zenlayer's external security posture.

External Network Assessment

1. Reconnaissance

The engagement began with reconnaissance on the external network to gather information about exposed assets. Testers enumerated publicly available IPs, open ports, running services, and DNS records. Subdomain enumeration was also conducted to uncover additional attack surfaces. Tools like Nmap, DNS reconnaissance utilities, and OSINT techniques were employed for mapping the attack surface.

2. Subdomain and DNS Testing

Subdomain enumeration and DNS record analysis were performed to identify misconfigurations or vulnerabilities, such as subdomain takeovers. Discovered subdomains hosting applications were included in the web application assessment for further testing.

3. Vulnerability Scanning

Automated scans were conducted to identify known vulnerabilities (CVE-based) in exposed services and software. Special attention was given to services like SSH, RDP, and VPN for misconfigurations, outdated versions, or weak encryption standards.

4. Exploitation of Network Services

Exploitation attempts focused on identified vulnerabilities, such as insecure configurations in SMB, FTP, or SNMP, and brute-forcing credentials for exposed administrative interfaces. The testers evaluated the external network for potential lateral movement scenarios or access to sensitive services.

5. Firewall and IDS/IPS Evasion

The testers assessed the effectiveness of firewall rules and intrusion detection systems by attempting to bypass them using evasion techniques. This included testing filtering mechanisms for misconfigurations or weaknesses.



6. Denial of Service (DoS)

Resilience against Denial of Service (DoS) attacks was tested to evaluate the infrastructure's ability to handle malformed traffic and prevent service degradation or outages.

Appendix A: Methodology

Testing Standard

Testing was conducted using a combination of frameworks and standards to comprehensively assess the security of Zenlayer, Inc.'s external network infrastructure.

- **External Network Security:** The testing adhered to the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, focusing on network-based security assessments.

Applicable Standards and Guidance

The penetration testing was conducted in compliance with the following:

- [NIST SP 800-53A](#): Assessing Security and Privacy Controls in Information Systems and Organizations, Revision 5, January 2022.
- [NIST SP 800-53](#): Security and Privacy Controls for Information Systems and Organizations, Revision 5, September 2020, with updates as of December 2020.
- [NIST 800-63-3](#): Digital Identity Guidelines, June 2017 with updates as of March 2020.
- [NIST SP 800-145](#): The NIST Definition of Cloud Computing, September 2011.
- [NIST SP 800-115](#): Technical Guide to Information Security Testing and Assessment, September 2008.

Summary of Methodology

The methodology focused on simulating real-world external attacker scenarios to evaluate the security posture of Zenlayer's internet-facing network infrastructure and exposed services. It included the following phases:

1. **Reconnaissance:** Information gathering on exposed assets, endpoints, and features.
2. **Vulnerability Assessment:** Automated and manual identification of security flaws.
3. **Exploitation:** Attempting to leverage identified vulnerabilities to gain unauthorized access or disrupt services.
4. **Post-Exploitation Analysis:** Evaluating the impact and extent of successful attacks.
5. **Reporting:** Providing actionable recommendations to mitigate identified risks.



Appendix B: Risk Rating

Quantitative Rating

The risk level of vulnerabilities has been calculated using the [Common Vulnerability Scoring System \(CVSS\) v4.0](#). CVSS is an open standard for describing the features and severity of software vulnerabilities. CVSS includes four metric groups: Base, Threat, Environmental, and Supplemental.

- **Base Metrics** capture the fundamental characteristics of a vulnerability that remain unchanged over time and across different environments.
- **Threat Metrics** account for the dynamic aspects of a vulnerability that may evolve.
- **Environmental Metrics** reflect the attributes of a vulnerability that are specific to an individual user's environment.

The Base metric values are combined with assumed maximum severity values for the Threat and Environmental metrics to calculate a score between 0 and 10. This score can be further refined by adjusting the Threat and Environmental metrics according to relevant threat intelligence and environmental factors.

- **Supplemental Metrics** provide additional insights into a vulnerability's characteristics but do not influence the final score. The CVSS vector string is a compressed text format that represents the values used to calculate the score.

Base Metrics [?]

Exploitability Metrics

Attack Vector (AV):	Network (N)	<input checked="" type="button" value="Adjacent (A)"/>	Local (L)	Physical (P)
Attack Complexity (AC):	<input checked="" type="button" value="Low (L)"/>	High (H)		
Attack Requirements (AT):	None (N)	<input checked="" type="button" value="Present (P)"/>		
Privileges Required (PR):	<input checked="" type="button" value="None (N)"/>	Low (L)	High (H)	
User Interaction (UI):	None (N)	<input checked="" type="button" value="Passive (P)"/>	Active (A)	

Vulnerable System Impact Metrics

Confidentiality (VC):	High (H)	Low (L)	<input checked="" type="button" value="None (N)"/>
Integrity (VI):	High (H)	<input checked="" type="button" value="Low (L)"/>	None (N)
Availability (VA):	<input checked="" type="button" value="High (H)"/>	Low (L)	None (N)

Subsequent System Impact Metrics

Confidentiality (SC):	High (H)	Low (L)	<input checked="" type="button" value="None (N)"/>
Integrity (SI):	<input checked="" type="button" value="High (H)"/>	Low (L)	None (N)
Availability (SA):	High (H)	<input checked="" type="button" value="Low (L)"/>	None (N)

Figure 1 - <https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator>



Qualitative Rating

In CVSS v4.0, the Qualitative Severity Rating Scale categorizes vulnerabilities based on their numerical scores to help organizations prioritize their response and remediation efforts. Here's a detailed description of each category:

Informational (0.0)	
Description	Action
A score of 0.0 indicates that the vulnerability has no impact on the security of the system. It represents scenarios where the vulnerability does not pose any risk or where the exploitability is practically impossible.	Typically, no immediate action is required as there is no security risk.

Low (0.1 to 3.9)	
Description	Action
Vulnerabilities classified as "Low" have a limited impact and are not considered a significant threat. They may require specific conditions to be exploited, or the impact of the exploitation is minimal.	These vulnerabilities are usually addressed in regular maintenance cycles but do not require urgent remediation.

Medium (4.0 to 6.9)	
Description	Action
"Medium" severity vulnerabilities have a moderate impact and are more likely to be exploited than low-severity ones. While they can cause some level of harm, they do not result in significant damage or breaches.	These should be addressed with moderate priority, especially if they are found in critical components of a system.



High (7.0 to 8.9)	
Description	Action
Vulnerabilities with a “High” rating pose a significant threat to the security of the system. They are easier to exploit and can lead to substantial damage, such as unauthorized access, data breaches, or system compromise.	These vulnerabilities should be addressed as a high priority to prevent potential exploitation, particularly in sensitive or critical systems.

Critical (9.0 to 10.0)	
Description	Action
“Critical” vulnerabilities represent the most severe threats, where exploitation is straightforward, and the impact is substantial, such as total system compromise, extensive data breaches, or a complete denial of service. These vulnerabilities are often exploitable remotely and can be automated.	Immediate action is required to mitigate these vulnerabilities as they pose a severe risk to the organization’s assets and operations. Rapid response and remediation are critical to minimize potential damage.

Risk Assessment Guidelines

Discloze conducted this penetration testing in conformity with [NIST SP 800-30 Rev 1](#) which provides a detailed framework for conducting risk assessments, focusing on three main components:

- **Threat Identification:** Determine potential threats that could exploit identified vulnerabilities, such as cyber-attacks, insider threats, or environmental factors.
- **Vulnerability Analysis:** Analyze how the identified vulnerabilities could be exploited by the threats, using information from CVSS scoring.
- **Impact Analysis:** Evaluate the potential impact of vulnerabilities if exploited, considering both the direct consequences on the affected system and the broader organizational impact, such as financial loss, reputational damage, or regulatory implications.



By integrating NIST SP 800-30 Rev 1, this framework ensures that the risk rating process not only assesses the technical severity (via CVSS) but also considers the broader risk context, including threat landscape and organizational impact.

Risk	CVSS Base Score	Severity Rating	Threat Analysis (NIST SP 800-30 Rev 1)	Impact Analysis	Recommended Action
Risk A	9.1	Critical	High likelihood of exploitation by remote attackers	High impact on operations and data security	Immediate patching and continuous monitoring
Risk B	5.4	Medium	Moderate likelihood of exploitation in targeted attacks	Moderate risk to data integrity	Prioritize for next patch cycle
Risk C	3.2	Low	Low likelihood; requires insider access	Minimal impact; low priority threat	Regular monitoring and review

References

- <https://www.first.org/cvss/v4-0/>
- <https://nvd.nist.gov/vuln-metrics/cvss>
- <https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator>

Appendix C: References

A01:2021 – Broken Access Control

- OWASP Top 10 2021: [Broken Access Control](#)
- OWASP Cheat Sheet: [Insecure Direct Object Reference Prevention Cheat Sheet](#)
- OWASP Cheat Sheet: [Transaction Authorization Cheat Sheet](#)
- OWASP Cheat Sheet: [Authorization Cheat Sheet](#)
- OWASP Cheat Sheet: [Cross-Site Request Forgery Prevention Cheat Sheet](#)

A02:2021 – Cryptographic Failures

- OWASP Top 10 2021: [Cryptographic Failures](#)
- Forgot Password: [Cheat Sheet](#)
- Session Management: [Cheat Sheet](#)
- Choosing and Using Security Questions [Cheat Sheet](#)
- Credential Stuffing [Cheat Sheet](#)
- Denial of Service [Cheat Sheet](#)
- JSON Web Token [Cheat Sheet](#)
- Multi-Factor Authentication [Cheat Sheet](#)
- Password Storage [Cheat Sheet](#)
- SAML Security [Cheat Sheet](#)
- API Security [Best Practices](#)

A03:2021 – Injection

- OWASP Top 10 2021: [Injection](#)
- Cross Site Scripting Prevention [Cheat Sheet](#)
- DOM Based XSS Prevention [Cheat Sheet](#)
- Content Security [Policy](#)

A04:2021 – Insecure Design

- OWASP Top 10 2021: [Insecure Design](#)
- OWASP Security Architecture: [Best Practices](#)
- ASVS Token Based Session Management [Cheat Sheet](#)
- Use of Strong Keys: [Guidelines](#)



A05:2021 – Security Misconfiguration

- OWASP Top 10 2021: [Security Misconfiguration](#)
- OWASP Top 10 2021: [Vulnerable and Outdated Components](#)
- [HTTP Strict Transport Security Cheat Sheet](#)
- [PHP Configuration Cheat Sheet](#)
- [XML External Entity Prevention Cheat Sheet](#)
- [Infrastructure as Code Security Cheat Sheet](#)

A06:2021 – Vulnerable and Outdated Components

- OWASP Top 10 2021: [Vulnerable and Outdated Component](#)
- OWASP: [Dependency-Check](#)
- OWASP: [Software Component Verification Standard \(SCVS\)](#)
- [Vulnerable Dependency Management Cheat Sheet](#)
- [Third Party JavaScript Management Cheat Sheet](#)
- [NPM Security Best Practices](#)
- [ImageMagick Zero Days](#)

A07:2021 – Identification and Authentication Failures

- OWASP Top 10 2021: [Identification and Authentication Failures](#)
- OWASP: [Authentication Cheat Sheet](#)
- OWASP: [Session Management Cheat Sheet](#)
- OWASP: [Password Storage Cheat Sheet](#)

A08:2021 – Software and Data Integrity Failures

- OWASP Top 10 2021: [Software and Data Integrity Failures](#)
- [CWE-79: Improper Neutralization of Input During Web Page Generation \(Cross-Site Scripting\)](#): [Definition](#)
- OWASP Configuration and Deployment Management: [Testing](#)
- [Stored XSS](#)
- [Protecting Java Applications: Cheat Sheet](#)
- OWASP Java: [Encoder](#)
- OWASP Java Encoder Additional: [Information](#)

A09:2021 – Security Logging and Monitoring Failures

- OWASP Top 10 2021: [Security Logging and Monitoring Failures](#)
- OWASP Proactive Controls: [Implement Logging and Monitoring](#)
- OWASP Application Security Verification Standard: [V7 Logging and Monitoring](#)



- OWASP Testing Guide: [Testing for Detailed Error Code](#)
- OWASP Cheat Sheet: [Application Logging Vocabulary](#)
- OWASP Cheat Sheet: [Logging](#)
- Data Integrity: [Recovering from Ransomware and Other Destructive Events](#)
- Data Integrity: [Identifying and Protecting Assets Against Ransomware and Other Destructive Events](#)
- Data Integrity: [Detecting and Responding to Ransomware and Other Destructive Events](#)

A10:2021 – Server-Side Request Forgery (SSRF)

- OWASP Top 10 2021: [Server-Side Request Forgery \(SSRF\)](#)
- OWASP Cheat Sheet: [Server-Side Request Forgery Prevention Cheat Sheet](#)
- OWASP Top 10 2021: [Security Logging and Monitoring Failures](#)



Document Tracking

Data Classification: CONFIDENTIAL

Version	Date	Author	Notes
1.0	01/06/2026	Tamer Mahmoud	Initial Draft
1.1	01/07/2026	Joseph Melika	Review
1.2	01/28/2026	Tamer Mahmoud	Deliver
1.3	01/28/2026	Tamer Mahmoud	Deliver
1.4	03/05/2026	Tamer Mahmoud	Deliver

Contact Information

Name	Title	Contact Information
Joseph Melika	CEO	joseph@discloze.com
Tamer Mahmoud	VP, Threat Intelligence	tm@discloze.com

