



TECHDEFENCELABS

Your Trusted **Cyber Security** Partner

A CERT-In Empanelled Information Security Organisation

No:- 3(15)/2004-CERT-In



Document Authorization, Revision History, and Control

Document Preparation	
Document Title	Internal Infrastructure Vulnerability Assessment and Penetration Testing Report
Evaluated Organization	LKP Securities Limited
Document ID	TDL-LSL-NG-04/26/0039
Report Version	v1.0
Assessment Approach	Grey Box Infrastructure VAPT Audit Report
Type of Audit Report	First Audit Report
Primary Assessment Period	06-Jan-2026 to 10-Feb-2026
Re-Assessment Period	Follow Up Audit Not Performed
Report Prepared by	Ayush Nandi
Reviewed by	Heet Kakadiya
Approved by	Rohit Soni
Released by	Pavan Saxena
Date of Release	15-Apr-2026

Document Change History		
Version	Date	Remarks / Reason of Change
v1.0	15-Apr-2026	First Audit Report

Document Distribution List			
Name	Organization	Designation	Email Id
Dhruv Chauhan	TechDefence Labs Pvt Ltd	Enterprise Business – Manager	dhruv.chauhan@techdefence.com
Umair Patel	LKP Securities Ltd	Asst. Manager – Information Security	umair.patel@lkpsec.com

Confidentiality and Disclaimer

This report is prepared exclusively for the management of the Evaluated organization and is intended solely for internal use. TechD Cybersecurity Limited disclaims any liability to third parties for the unauthorized use or distribution of this document or its contents. The findings, information, data, advice, and recommendations are based on the cooperation of the Evaluated organization and the data provided during the assessment period. Any limitations due to environmental constraints, access restrictions, or insufficient information may have impacted the thoroughness of our analysis and could result in unidentified vulnerabilities.

The report assesses the initial security controls implemented by the Evaluated organization, specifically focusing on the security of the defined domain and systems in-scope. TechD Cybersecurity Limited highlights areas for potential improvement; however, the responsibility for implementing and maintaining robust security measures lies with the management of the Evaluated organization. The information provided in this document reflects the state of the security environment at the time of preparation and is not an exhaustive evaluation.

Note: *For the purpose of this report, the term “Evaluated organization” refers to the client organization for which this assessment was conducted.*

©TechD Cybersecurity Limited, 2026
9th Floor, Abhishree Adroit,
Near Mansi Circle, Vastrapur,
Ahmedabad-380015.

Table of Contents

Document Authorization, Revision History, and Control	2
Document Preparation	2
Document Change History	2
Document Distribution List	2
Confidentiality and Disclaimer	3
1. Assessment Details	5
1.1 Engagement Scope	5
1.2 Scope Exclusions	7
1.3 Project Team	7
1.4 Tools used during the assessment	8
2. VAPT Audit Methodology and Standards	9
2.1 Phases of the Assessment	9
2.2 Standards and Methodologies	9
2.3 Vulnerability Risk Rating Metrics and Remediation SLA	10
3. Executive Summary	11
3.1 Visual Representation of Assessment Results	11
4. Detailed Vulnerability Observations	12
Annexure A - Engagement Limitations	37
Annexure B - Retesting Statement	37
Annexure C - Disclaimer and Precautions for Patch Implementation	38
Annexure D - CERT-In Reporting and Remediation Compliance	38

1. Assessment Details

The evaluated organization engaged TechD Cybersecurity Limited to assess the security of its infrastructure. The evaluation focused on identifying infrastructure-level vulnerabilities, testing security mechanisms, and resilience against unauthorized access. The assessment followed industry standards, including NIST 800-115 and Penetration Testing Execution Standard (PTES).

1.1 Engagement Scope

The following Infrastructure IPs provided by the Evaluated organization were identified as in scope for this security assessment, as defined during the engagement.

In Scope of Assessment			
Type of Infrastructure	IP Address	No. of Devices	Internal/External
Server	172.17.100.31	34	Internal
	172.17.100.32		
	172.17.100.33		
	172.17.100.60		
	172.17.100.120		
	172.17.100.83		
	172.17.100.112		
	172.17.100.20		
	192.168.10.20		
	172.17.100.56		
	172.17.100.59		
	172.17.100.35		
	172.17.100.73		
	172.17.100.66		
	172.17.100.151		
	172.17.100.177		
	172.17.100.152		
	172.17.100.53		
	172.17.100.81		
	172.17.100.68		
	172.17.100.54		
	172.17.100.145		
	172.17.100.146		
	172.17.100.147		
	172.17.100.148		
	172.17.100.38		

	172.17.100.232 172.17.100.233 172.17.100.234 172.17.100.235 172.17.100.236 172.17.100.237 172.17.100.141 172.17.100.140		
Endpoints	192.168.150.180 192.168.150.166 192.168.150.115 192.168.10.85 192.168.10.134 192.168.150.71 192.168.150.238 192.168.150.74 192.168.10.184 192.168.150.133 192.168.10.127 192.168.10.80 192.168.10.194 192.168.150.66 192.168.150.199 192.168.150.139 192.168.150.9 192.168.150.29 192.168.150.64 192.168.150.148	20	Internal
Firewall	172.17.100.98 172.17.100.99	2	Internal
Switch	172.17.100.10 172.17.100.101	2	Internal

1.2 Scope Exclusions

1. Security assessment or Vulnerability Assessment and Penetration Testing (VAPT) of applications hosted on systems within the scoped IP range is outside the scope of this network VAPT engagement unless explicitly specified.
2. Detailed configuration reviews or hardening assessments of network devices (e.g., firewalls, routers, switches) are excluded unless specifically included within the scope.
3. For production environments, any test cases or activities that may cause service disruption, instability, or downtime will be avoided during the assessment.
4. Exploitation of identified vulnerabilities will be limited to proof-of-concept (PoC) validation only. Full exploitation or actions that may impact system availability or integrity will not be performed.
5. Any IP addresses, network segments, systems, or management interfaces not explicitly provided or approved by the Evaluated organization will be considered out of scope.

1.3 Project Team

Below are the TechD Cybersecurity Limited Auditing team members who played a key role in this engagement:

Name	Designation	Email-ID	Qualifications/ Certifications	Listed in CERT-In Snapshot? (Yes/No)
Pavan Saxena	Team Lead - VAPT	pavan@techdefence.com	BCA OSCP, (ISC)2 - CC, AZ-900, CEHv12, eJPT-v2, CAP, CNSP, CAPen, KLCP, ISO-27001: Lead Auditor	Yes
Rushikesh Patil	Sr. Security Analyst	Rushikesh.patil@techdefence.com	CEH Master, ISO27001	No
Kunal Patil	Security Analyst	kunal.p@techdefence.com	BSc, CAP, CNSP	No

1.4 Tools used during the assessment

Sr. No	Name of Tool /Software used	Version of the tool /Software used	Open Source /Licensed
01	Nessus Professional	v10.11.3	Licensed
02	Nmap	v7.96	Open Source

2. VAPT Audit Methodology and Standards

2.1 Phases of the Assessment

- **Pre-engagement Phase:** This is the stage where the logistics and the rules of engagement of the test are discussed.
- **Reconnaissance/ Discovery Phase:** To simulate a cyber-attack on a infrastructure, the penetration tester needs access to information about the target. They gather this information in the reconnaissance stage.
- **Vulnerability Analysis:** This phase consists of testing the infrastructure for known vulnerabilities. Using an automated and manual approach for uncovering new and hidden vulnerabilities on the infrastructure.
- **Exploitation and Post Exploitation:** The goal here is establishing access to a system using the loopholes uncovered in the earlier phases of Pen testing. The penetration tester tries to identify an entry point and then look for assets that can be accessed through that.
- **Reporting and Recommendations:** All the previous penetration testing phases contribute to this phase where a VAPT report is created and shared with the client.
- **Remediation and Rescan:** Once the vulnerabilities are fixed, we would carry out the round of rescans to identify any security loopholes that might have been left unattended.

2.2 Standards and Methodologies

- **National Institute of Standards and Technology - NIST 800-115:** NIST 800-115 provides guidelines for conducting structured information security testing and assessments, focusing on vulnerability scanning, penetration testing, and overall security evaluations. The methodology involves assessing the organization's network infrastructure, identifying vulnerabilities, and generating detailed reports with actionable recommendations. Emphasizing continuous improvement, it ensures a systematic approach to strengthening network security through effective testing and mitigation strategies.
- **Penetration Testing Execution Standard (PTES):** The Penetration Testing Execution Standard (PTES) provides a structured methodology for conducting comprehensive penetration testing. It includes seven essential phases—planning, information gathering, threat modelling, vulnerability analysis, exploitation, post-exploitation, and reporting—ensuring thorough coverage of vulnerabilities and helping organizations enhance their security posture through systematic testing and analysis.

2.3 Vulnerability Risk Rating Metrics and Remediation SLA

This section outlines the methodology used to assess and classify vulnerabilities based on the Common Vulnerability Scoring System (CVSS), along with the corresponding risk ratings. In addition, it defines the recommended remediation timelines for identified vulnerabilities based on their severity and potential business impact.

The Recommended Remediation Timelines provided in this report are suggested by TechD Cybersecurity Limited, based on industry best practices, risk exposure, and experience from similar engagements. These timelines are intended to assist the Evaluated organization in prioritizing remediation efforts effectively and reducing overall security risk.

Risk Exposure	CVSS Score	Remediation Timeline	Description
Critical	9.0 – 10.0	Within 7 Days	Immediate risk of severe impact on confidentiality, integrity, or availability.
High	7.0 – 8.9	Within 15 Days	High risk of system or data compromise requiring urgent remediation.
Medium	4.0 – 6.9	Within 30 Days	Moderate risk with potential for exploitation under certain conditions.
Low	0.1 – 3.9	Within 60 Days	Low risk with limited impact and specific exploitation requirements.
Informational	0	As per Business Priority	No direct risk; improvement recommendations for security posture.

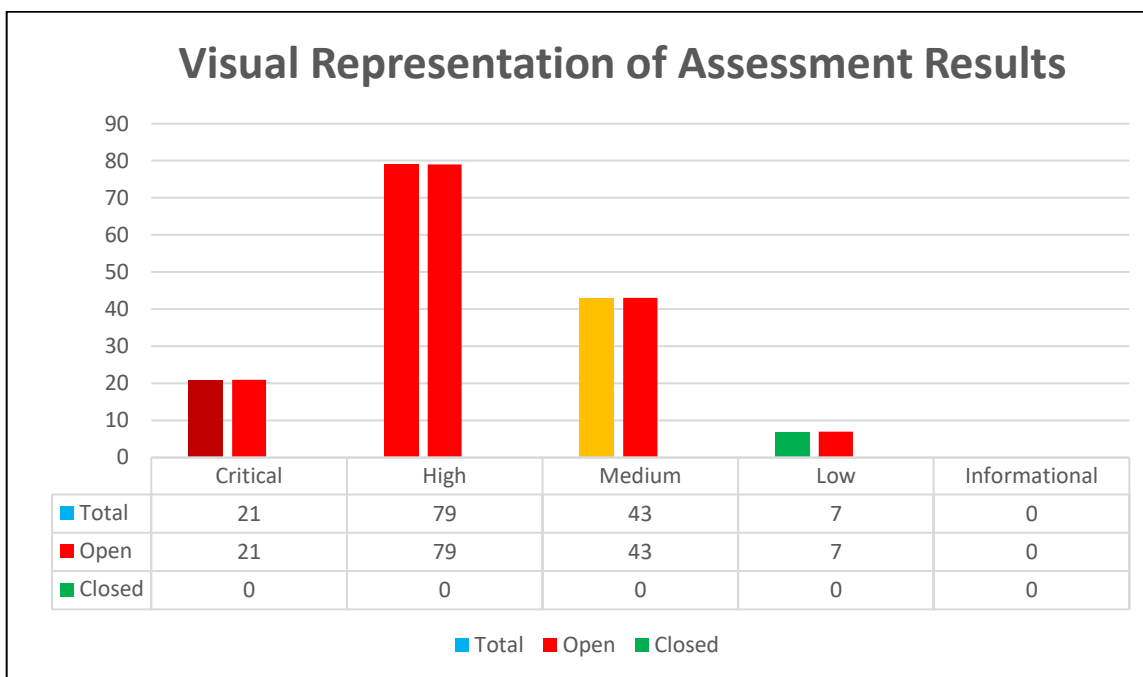
Risk Factors: Risk is assessed based on two primary factors: Likelihood and Impact.

- **Likelihood:** This factor measures the probability of a vulnerability being exploited. Ratings are determined by the attack difficulty, the availability of tools, the skill level of potential attackers, and the environment.
- **Impact:** This factor evaluates the potential consequences of a vulnerability on operations, including its effect on confidentiality, integrity, and availability of systems/data, as well as any reputational or financial damage.

3. Executive Summary

The following section provides an Executive Summary of the vulnerabilities identified during this Security Audit. Detailed recommendations for each observation are outlined in Section 4 of this report.

3.1 Visual Representation of Assessment Results



4. Detailed Vulnerability Observations

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
TDL-001	192.168.10.134, 192.168.150.133, 192.168.10.127, 192.168.150.9, 172.17.100.38, 172.17.100.60, 172.17.100.112, 172.17.100.146, 172.17.100.148, 172.17.100.177	Microsoft ASP.NET Core Security Feature Bypass (October 2025)	CVE-2025-55315	Critical	Open
TDL-002	192.168.150.133, 192.168.150.148, 192.168.150.180, 192.168.10.127, 192.168.150.9, 172.17.100.60, 172.17.100.73, 172.17.100.112, 172.17.100.120	Microsoft Office Unsupported Version Detection	N/A	Critical	Open
TDL-003	192.168.150.133, 192.168.150.71	Google Chrome < 143.0.7499.146 Multiple Vulnerabilities	CVE-2025-14766	Critical	Open
TDL-004	192.168.150.148, 192.168.150.199, 192.168.10.80, 192.168.10.127, 192.168.10.184, 192.168.150.9, 192.168.150.29, 192.168.150.71, 192.168.150.115, 192.168.150.139, 192.168.150.166, 192.168.150.238, 172.17.100.60, 172.17.100.83, 172.17.100.112,	Microsoft .NET Core SEoL	N/A	Critical	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.146, 172.17.100.120, 172.17.100.140, 172.17.100.148, 172.17.100.177				
TDL-005	192.168.10.127	Microsoft Internet Explorer Unsupported Version Detection	N/A	Critical	Open
TDL-006	192.168.10.127	Microsoft Windows 10 20H2 Pro SEoL	N/A	Critical	Open
TDL-007	192.168.150.166, 172.17.100.33, 172.17.100.120	Kaspersky Endpoint Security Detection and Status	N/A	Critical	Open
TDL-008	192.168.150.166, 172.17.100.20, 172.17.100.38, 172.17.100.60, 172.17.100.73, 192.168.10.20, 172.17.100.68, 172.17.100.112, 172.17.100.120, 172.17.100.141, 172.17.100.177	Apache Log4j SEoL (<= 1.x)	CVE-2023-26464	Critical	Open
TDL-009	192.168.150.238, 172.17.100.35	Microsoft Silverlight SEoL	N/A	Critical	Open
TDL-010	172.17.100.232, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237, 172.17.100.233	VMware ESXi 7.x < 7.0 Update 3w / 8.x < 8.0 Update 2e / 8.0 Update 3 < 8.0 Update 3f (VMSA-2025-0013)	CVE-2025-41239	Critical	Open
TDL-011	172.17.100.54	Redis Server Unprotected by Password Authentication	N/A	Critical	Open
TDL-012	172.17.100.60, 172.17.100.73, 172.17.100.112	Microsoft SQL Server Unsupported Version Detection	N/A	Critical	Open
TDL-013	172.17.100.60, 172.17.100.83,	.NET Core SDK SEoL	N/A	Critical	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.112, 172.17.100.120				
TDL-014	172.17.100.60, 172.17.100.83, 172.17.100.112, 172.17.100.146, 172.17.100.120, 172.17.100.140, 172.17.100.148, 172.17.100.177	ASP.NET Core SEoL	N/A	Critical	Open
TDL-015	172.17.100.151	Mozilla Foundation Unsupported Application Detection	N/A	Critical	Open
TDL-016	172.17.100.53, 172.17.100.68	Microsoft Message Queuing RCE (CVE-2023-21554, QueueJumper)	CVE-2023-21554	Critical	Open
TDL-017	172.17.100.81	SSL Version 2 and 3 Protocol Detection	N/A	Critical	Open
TDL-018	172.17.100.83	Adobe Flash Player Unsupported Version Detection	N/A	Critical	Open
TDL-019	172.17.100.33	Git for Windows < 2.45.1 Multiple Vulnerabilities	CVE-2024-32465	Critical	Open
TDL-020	172.17.100.33	Wireshark SEoL (2.0.x)	N/A	Critical	Open
TDL-021	172.17.100.120	Oracle MySQL Connectors (October 2024 CPU)	CVE-2024-6119	Critical	Open
TDL-022	192.168.10.85, 192.168.10.134, 192.168.150.133, 192.168.150.180, 192.168.10.127, 192.168.150.71, 192.168.150.115, 192.168.150.166, 192.168.150.238, 172.17.100.31, 172.17.100.38, 172.17.100.73, 192.168.10.20, 172.17.100.53,	Microsoft Windows Unquoted Service Path Enumeration	CVE-2014-5455	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.68, 172.17.100.152				
TDL-023	192.168.10.85, 192.168.10.134, 192.168.10.194, 192.168.150.66, 192.168.150.74, 172.17.100.38, 172.17.100.60, 172.17.100.140	MS16-029: Security Update for Microsoft Office to Address Remote Code Execution (3141806)	CVE-2016-0134	High	Open
TDL-024	192.168.10.85, 192.168.10.134, 192.168.10.194, 192.168.150.66, 172.17.100.38, 172.17.100.60, 172.17.100.140	MS17-014: Security Update for Microsoft Office (4013241)	CVE-2017-0107	High	Open
TDL-025	192.168.10.85, 192.168.10.134, 192.168.10.194, 192.168.150.66, 172.17.100.60	Security Update for Microsoft Office Excel Products (September 2017)	CVE-2017-8632	High	Open
TDL-026	192.168.10.85, 192.168.150.74, 172.17.100.38, 172.17.100.60	Security Feature Bypass Vulnerability for Microsoft Excel Products (June 2020)	CVE-2020-1226	High	Open
TDL-027	192.168.10.85, 192.168.10.134, 192.168.150.133, 192.168.150.148, 192.168.150.180, 192.168.10.127, 192.168.10.194, 192.168.150.9, 192.168.150.66, 192.168.150.74, 192.168.150.115, 192.168.150.166,	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)	CVE-2013-3900	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.20, 172.17.100.31, 172.17.100.32, 172.17.100.38, 172.17.100.59, 172.17.100.60, 172.17.100.73, 172.17.100.151, 192.168.10.20, 172.17.100.53, 172.17.100.68, 172.17.100.81, 172.17.100.83, 172.17.100.112, 172.17.100.152, 172.17.100.146, 172.17.100.147, 172.17.100.33, 172.17.100.35, 172.17.100.120, 172.17.100.140, 172.17.100.148, 172.17.100.141, 172.17.100.66, 172.17.100.177, 172.17.100.145				
TDL-028	192.168.10.85, 192.168.10.134, 192.168.10.194, 192.168.150.66, 192.168.150.74, 172.17.100.38, 172.17.100.140	Security Updates for Microsoft OneNote Products (April 2025)	CVE-2025-29822	High	Open
TDL-029	192.168.10.85, 192.168.10.134, 192.168.10.194, 192.168.150.66, 192.168.150.74,	Security Updates for Outlook (July 2025)	CVE-2025-49699	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.38, 172.17.100.35, 172.17.100.140				
TDL-030	192.168.10.85, 192.168.10.134, 192.168.10.194, 192.168.150.66, 192.168.150.74, 172.17.100.38, 172.17.100.35, 172.17.100.140	Security Updates for Microsoft PowerPoint Products (October 2025)	CVE-2025-59238	High	Open
TDL-031	192.168.10.85, 192.168.10.134, 192.168.10.194, 192.168.150.66, 192.168.150.74, 172.17.100.38, 172.17.100.35, 172.17.100.140	Security Updates for Microsoft Office Products (December 2025)	CVE-2025-62563	High	Open
TDL-032	192.168.10.85, 192.168.10.134, 192.168.10.194, 192.168.150.66, 192.168.150.74, 172.17.100.38, 172.17.100.35, 172.17.100.140	Security Updates for Microsoft Word Products (December 2025)	CVE-2025-62562	High	Open
TDL-033	192.168.10.85, 192.168.10.134, 192.168.10.194, 192.168.150.66, 192.168.150.74, 172.17.100.38, 172.17.100.35, 172.17.100.140	Security Updates for Microsoft Excel Products (December 2025)	CVE-2025-62564	High	Open
TDL-034	192.168.10.134, 192.168.10.194, 172.17.100.31,	MS09-035: Vulnerabilities in Visual Studio Active Template Library	CVE-2009-2495	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.56, 172.17.100.59, 172.17.100.53, 172.17.100.68, 172.17.100.81	Could Allow Remote Code Execution (969706)			
TDL-035	192.168.10.134, 192.168.150.133, 192.168.150.180, 192.168.150.199, 192.168.10.80, 192.168.10.127, 192.168.10.184, 192.168.10.194, 192.168.150.9, 192.168.150.29, 192.168.150.115, 192.168.150.166, 192.168.150.238, 172.17.100.31, 172.17.100.32, 172.17.100.38, 172.17.100.56, 172.17.100.59, 172.17.100.73, 192.168.10.20, 172.17.100.53, 172.17.100.68, 172.17.100.81, 172.17.100.146, 172.17.100.147, 172.17.100.33, 172.17.100.35, 172.17.100.120, 172.17.100.140, 172.17.100.148, 172.17.100.141, 172.17.100.66, 172.17.100.145	SSL Medium Strength Cipher Suites Supported (SWEET32)	CVE-2016-2183	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
TDL-036	192.168.10.134, 172.17.100.38, 172.17.100.140	Security Update for Microsoft Office Products (July 2017)	CVE-2017-8570	High	Open
TDL-037	192.168.10.134, 192.168.150.139	Microsoft Office Protected View Disabled	N/A	High	Open
TDL-038	192.168.10.134, 192.168.150.133, 192.168.150.148, 192.168.150.180, 192.168.10.127, 192.168.10.194, 192.168.150.9, 192.168.150.66, 192.168.150.115, 192.168.150.166, 172.17.100.20, 172.17.100.38, 172.17.100.56, 172.17.100.59, 172.17.100.60, 172.17.100.73, 192.168.10.20, 172.17.100.81, 172.17.100.83, 172.17.100.112, 172.17.100.33, 172.17.100.35, 172.17.100.120, 172.17.100.177	WinRAR < 7.00 Multiple Vulnerabilities	CVE-2024-36052	High	Open
TDL-039	192.168.10.134	Oracle Java (Apr 2024 CPU)	CVE-2024-21892	High	Open
TDL-040	192.168.10.134, 192.168.10.194, 192.168.150.66, 172.17.100.38, 172.17.100.140	Security Updates for Microsoft Publisher Products (September 2024)	CVE-2024-38226	High	Open
TDL-041	192.168.10.134	Oracle VM VirtualBox (July 2025 CPU)	CVE-2025-53030	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
TDL-042	192.168.10.134, 192.168.150.133, 192.168.150.148, 192.168.150.180, 192.168.150.199, 192.168.10.80, 192.168.10.127, 192.168.10.184, 192.168.10.194, 192.168.150.9, 192.168.150.29, 192.168.150.66, 192.168.150.71, 192.168.150.115, 192.168.150.139, 192.168.150.166, 192.168.150.238, 172.17.100.20, 172.17.100.31, 172.17.100.32, 172.17.100.38, 172.17.100.56, 172.17.100.59, 172.17.100.60, 172.17.100.73, 192.168.10.20, 172.17.100.68, 172.17.100.81, 172.17.100.83, 172.17.100.112, 172.17.100.152, 172.17.100.146, 172.17.100.147, 172.17.100.33, 172.17.100.35, 172.17.100.120, 172.17.100.148,	RARLAB WinRAR < 7.13 Directory Traversal (CVE-2025-8088)	CVE-2025-8088	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.177, 172.17.100.145				
TDL-043	192.168.10.134, 192.168.150.29, 192.168.150.166, 172.17.100.60, 172.17.100.73, 172.17.100.112, 172.17.100.35	Oracle Java SE Multiple Vulnerabilities (October 2025 CPU)	CVE-2025-6558	High	Open
TDL-044	192.168.10.134, 192.168.150.133, 192.168.150.148, 192.168.150.180, 192.168.150.199, 192.168.10.80, 192.168.10.184, 192.168.10.194, 192.168.150.9, 192.168.150.29, 192.168.150.115, 192.168.150.139, 192.168.150.166, 192.168.150.238, 172.17.100.35	KB5071546: Windows 10 version 21H2 / Windows 10 Version 22H2 Security Update (December 2025)	CVE-2025-64673	High	Open
TDL-045	192.168.150.148, 172.17.100.146, 172.17.100.140	Wireshark 4.4.x < 4.4.9 Multiple Vulnerabilities	CVE-2025-9817	High	Open
TDL-046	192.168.150.148, 192.168.150.199, 192.168.10.127, 192.168.150.9, 192.168.150.139, 172.17.100.151, 172.17.100.35	Mozilla Firefox < 146.0.1	CVE-2025-14861	High	Open
TDL-047	192.168.10.127	Security Update for .NET Core (June 2023)	CVE-2025-14861	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
TDL-048	192.168.10.127, 192.168.10.194, 172.17.100.35	Microsoft Paint 3D Code Execution (July 2023)	CVE-2023-35374	High	Open
TDL-049	192.168.10.127	Microsoft 3D Viewer app Multiple Remote Code Execution Vulnerabilities (September 2023)	CVE-2023-36760	High	Open
TDL-050	192.168.10.127, 192.168.10.194	Adobe Reader < 20.005.30838 / 25.001.20997 Multiple Vulnerabilities (APSB25-119)	CVE-2025-64899	High	Open
TDL-051	192.168.10.184	Ivanti Secure Access Client < 22.6R1.1 Multiple Vulnerabilities	CVE-2023-38543	High	Open
TDL-052	192.168.10.184	Ivanti Secure Access 22.x Multiple Vulnerabilities	CVE-2023-46810	High	Open
TDL-053	192.168.10.184	Cisco Webex App Client-Side RCE (cisco-sa-webex-app-client-rce- ufyMMYLC)	CVE-2025-20236	High	Open
TDL-054	192.168.10.194	MS15-099: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3089664)	CVE-2015-2545	High	Open
TDL-055	192.168.150.29	Microsoft Office Trust Access to VBA Project Model Object Enabled	N/A	High	Open
TDL-056	192.168.150.66	Dell Client BIOS Multiple Vulnerabilities (DSA-2022-224)	CVE-2022-26861	High	Open
TDL-057	192.168.150.74	VLC < 3.0.18 Multiple Vulnerabilities	CVE-2022-41325	High	Open
TDL-058	192.168.150.115, 172.17.100.20, 172.17.100.31, 172.17.100.32, 172.17.100.56, 172.17.100.59, 192.168.10.20, 172.17.100.53, 172.17.100.68, 172.17.100.83, 172.17.100.112, 172.17.100.33, 172.17.100.148,	Security Updates for Microsoft .NET Framework (January 2025)	CVE-2025-21176	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.177, 172.17.100.145				
TDL-059	192.168.150.166, 192.168.150.238, 172.17.100.81, 172.17.100.152, 172.17.100.120, 172.17.100.140	Insecure Windows Service Permissions	N/A	High	Open
TDL-060	192.168.150.166, 192.168.10.20	Node.js Multiple Vulnerabilities (November 2018 Security Releases)	CVE-2018-5407	High	Open
TDL-061	192.168.150.238	MS16-109: Security Update for Silverlight (3182373)	CVE-2018-5407	High	Open
TDL-062	192.168.150.238, 172.17.100.60	MS17-013: Security Update for Microsoft Graphics Component (4013075)	CVE-2018-5407	High	Open
TDL-063	172.17.100.54	RHEL 9 : webkit2gtk3 (RHSA-2025:23700)	CVE-2025-43541	High	Open
TDL-064	172.17.100.20, 172.17.100.38, 172.17.100.56, 172.17.100.59, 172.17.100.60, 172.17.100.68, 172.17.100.83, 172.17.100.112, 172.17.100.147, 172.17.100.33, 172.17.100.35, 172.17.100.120, 172.17.100.177, 172.17.100.145	Microsoft Azure Data Studio < 1.48.0 Elevation of Privilege Vulnerability (CVE-2024-26203)	CVE-2024-26203	High	Open
TDL-065	172.17.100.20, 172.17.100.38, 172.17.100.56, 172.17.100.59, 172.17.100.60, 172.17.100.73, 192.168.10.20,	Security Updates for Microsoft SQL Server (November 2025)	CVE-2025-59499	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.68, 172.17.100.83, 172.17.100.112, 172.17.100.147, 172.17.100.120, 172.17.100.141, 172.17.100.177, 172.17.100.145				
TDL-066	172.17.100.20, 172.17.100.38, 172.17.100.56, 172.17.100.59, 172.17.100.60, 172.17.100.73, 172.17.100.68, 172.17.100.83, 172.17.100.112, 172.17.100.147, 172.17.100.120, 172.17.100.141, 172.17.100.177, 172.17.100.145	Visual Studio Tools for Applications Elevation of Privilege (CVE-2025- 29803)	CVE-2025-29803	High	Open
TDL-067	172.17.100.20, 172.17.100.31, 172.17.100.32, 172.17.100.38, 172.17.100.56, 172.17.100.59, 192.168.10.20, 172.17.100.53, 172.17.100.68, 172.17.100.81, 172.17.100.83, 172.17.100.112, 172.17.100.146, 172.17.100.147, 172.17.100.33, 172.17.100.140,	KB5071544: Windows 10 version 1809 / Windows Server 2019 Security Update (December 2025)	CVE-2025-64673	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.148, 172.17.100.141, 172.17.100.66, 172.17.100.177, 172.17.100.145				
TDL-068	172.17.100.31, 172.17.100.60, 172.17.100.73, 172.17.100.81, 172.17.100.83, 172.17.100.146, 172.17.100.33, 172.17.100.35, 172.17.100.120, 172.17.100.148	Notepad++ < 8.8.2 Privilege Escalation (CVE-2025-49144)	CVE-2025-49144	High	Open
TDL-069	172.17.100.32	Security Update for Microsoft Visual Studio Code Python Extension (July 2025)	CVE-2025-49714	High	Open
TDL-070	172.17.100.38, 172.17.100.60	Microsoft Web Deploy < 10.0.2001 Remote Code Execution (CVE-2025-53772)	CVE-2025-53772	High	Open
TDL-071	172.17.100.38, 172.17.100.56, 172.17.100.59, 172.17.100.60, 172.17.100.151, 172.17.100.53, 172.17.100.68, 172.17.100.81, 172.17.100.112, 172.17.100.152, 172.17.100.146, 172.17.100.147, 172.17.100.35, 172.17.100.120, 172.17.100.140, 172.17.100.148, 172.17.100.141,	VMware Tools 11.x < 12.5.4 / 13.x < 13.0.5 Multiple Vulnerabilities (VMSA-2025-0015)	CVE-2025-41246	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.66, 172.17.100.177, 172.17.100.145				
TDL-072	172.17.100.56, 172.17.100.151, 172.17.100.112	Curl 7.84 <= 8.2.1 Header DoS (CVE-2023-38039)	CVE-2023-38039	High	Open
TDL-073	172.17.100.60	Oracle Database Multiple Vulnerabilities (April 2012 CPU)	CVE-2012-1708	High	Open
TDL-074	172.17.100.60	MS14-017: Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (2949660)	CVE-2014-1761	High	Open
TDL-075	172.17.100.60	MS14-081: Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3017301)	CVE-2014-6357	High	Open
TDL-076	172.17.100.60	Security Updates for Microsoft Publisher Products (April 2020)	CVE-2020-0760	High	Open
TDL-077	172.17.100.60	Security Updates for Microsoft PowerPoint Products (March 2021)	CVE-2021-27056	High	Open
TDL-078	172.17.100.60	Security Updates for Outlook (April 2021)	CVE-2021-28452	High	Open
TDL-079	172.17.100.60	Security Updates for Microsoft Excel Products (April 2021)	CVE-2021-28456	High	Open
TDL-080	172.17.100.60	Security Updates for Microsoft Office Products (April 2021)	CVE-2021-28454	High	Open
TDL-081	172.17.100.60	Security Updates for Microsoft Word Products (April 2021)	CVE-2021-28453	High	Open
TDL-082	172.17.100.60, 172.17.100.177	Security Update for Microsoft ASP.NET Core (February 2024) (CVE-2024-21386)	CVE-2024-21386	High	Open
TDL-083	172.17.100.60, 172.17.100.73, 172.17.100.120	KB5071543: Windows 10 Version 1607 / Windows Server 2016 Security Update (December 2025)	CVE-2025-64661	High	Open
TDL-084	172.17.100.73, 172.17.100.112	Microsoft Office Service Pack Out of Date	N/A	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
TDL-085	172.17.100.73	MS13-085: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2885080)	CVE-2013-3890	High	Open
TDL-086	172.17.100.73, 172.17.100.112	MS14-061: Vulnerability in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3000434)	CVE-2014-4117	High	Open
TDL-087	172.17.100.73, 172.17.100.141	Security Updates for SQL Server Management Studio (April 2025)	CVE-2025-29803	High	Open
TDL-088	172.17.100.73	Apache Tomcat 9.0.40 < 9.0.109 multiple vulnerabilities	CVE-2025-55754	High	Open
TDL-089	172.17.100.151	KB5044280: Windows 11 version 21H2 Security Update (October 2024)	CVE-2024-6197	High	Open
TDL-090	172.17.100.151	Security Updates for Microsoft .NET Framework (October 2024)	CVE-2024-43484	High	Open
TDL-091	192.168.10.20	Windows Defender Antimalware/Antivirus Signature Definition Check	N/A	High	Open
TDL-092	172.17.100.53	Security Updates for Microsoft .NET Framework (February 2023)	CVE-2023-21808	High	Open
TDL-093	172.17.100.81	Security Updates for Microsoft SQL Server ODBC Driver (April 2024)	CVE-2024-29043	High	Open
TDL-094	172.17.100.83	Adobe Flash Player <= 32.0.0.433 (APSB20-58)	CVE-2020-9746	High	Open
TDL-095	172.17.100.112, 172.17.100.177	Security Updates for Microsoft ASP.NET Core (October 2023)	CVE-2023-44487	High	Open
TDL-096	172.17.100.112, 172.17.100.177	Security Updates for Microsoft Visual Studio Products (July 2025)	CVE-2025-49739	High	Open
TDL-097	172.17.100.33	Security Updates for Microsoft SQL Server OLE DB Driver (July 2024)	CVE-2024-37334	High	Open
TDL-098	172.17.100.33	Mozilla Thunderbird < 140.6	CVE-2025-14333	High	Open
TDL-099	172.17.100.120	Security Updates for Microsoft .NET Core (December 2022)	CVE-2022-41089	High	Open
TDL-100	172.17.100.120	Security Updates for Microsoft ASP.NET Core (December 2022)	CVE-2022-41089	High	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
TDL-101	192.168.10.134, 192.168.150.180, 192.168.150.199, 192.168.10.80, 192.168.10.127, 192.168.10.194, 192.168.150.9, 192.168.150.64, 192.168.150.74, 192.168.150.139, 192.168.150.166, 192.168.150.66, 192.168.150.71, 172.17.100.20, 172.17.100.38, 172.17.100.59, 172.17.100.60, 172.17.100.73, 172.17.100.151, 192.168.10.20, 172.17.100.53, 172.17.100.68, 172.17.100.81, 172.17.100.83, 172.17.100.112, 172.17.100.146, 172.17.100.147, 172.17.100.120, 172.17.100.140, 172.17.100.148, 172.17.100.141, 172.17.100.66, 172.17.100.177, 172.17.100.145	SMB Signing not required	N/A	Medium	Open
TDL-102	192.168.10.134, 192.168.150.133, 192.168.150.180, 192.168.150.199,	TLS Version 1.0 Protocol Detection	N/A	Medium	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	192.168.10.85, 192.168.10.80, 192.168.10.127, 192.168.10.184, 192.168.10.194, 192.168.150.9, 192.168.150.29, 192.168.150.74, 192.168.150.115, 192.168.150.166, 192.168.150.238, 192.168.150.66, 192.168.150.71, 172.17.100.31, 172.17.100.32, 172.17.100.38, 172.17.100.56, 172.17.100.59, 172.17.100.73, 192.168.10.20, 172.17.100.53, 172.17.100.68, 172.17.100.81, 172.17.100.152, 172.17.100.146, 172.17.100.147, 172.17.100.33, 172.17.100.35, 172.17.100.120, 172.17.100.140, 172.17.100.148, 172.17.100.141, 172.17.100.66, 172.17.100.145				
TDL-103	192.168.10.134, 192.168.10.85, 192.168.10.194, 192.168.150.74,	Security Feature Bypass Vulnerability for Word (June 2020)	CVE-2020-1229	Medium	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	192.168.150.66, 172.17.100.38, 172.17.100.60, 172.17.100.140				
TDL-104	192.168.10.134	Oracle Java SE 1.7.0_331 / 1.8.0_321 / 1.11.0_14 / 1.17.0_2 Multiple Vulnerabilities (January 2022 CPU)	CVE-2022-21366	Medium	Open
TDL-105	192.168.10.134, 192.168.150.133, 192.168.150.180, 192.168.150.199, 192.168.10.85, 192.168.10.80, 192.168.10.127, 192.168.10.184, 192.168.10.194, 192.168.150.9, 192.168.150.29, 192.168.150.74, 192.168.150.115, 192.168.150.166, 192.168.150.238, 192.168.150.66, 192.168.150.71, 172.17.100.31, 172.17.100.32, 172.17.100.38, 172.17.100.56, 172.17.100.59, 172.17.100.73, 192.168.10.20, 172.17.100.53, 172.17.100.68, 172.17.100.81, 172.17.100.152, 172.17.100.146, 172.17.100.147,	TLS Version 1.1 Deprecated Protocol	N/A	Medium	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.33, 172.17.100.35, 172.17.100.120, 172.17.100.140, 172.17.100.148, 172.17.100.141, 172.17.100.66, 172.17.100.145				
TDL-106	192.168.10.134, 192.168.10.127, 192.168.150.9, 172.17.100.38, 172.17.100.60, 172.17.100.112, 172.17.100.146, 172.17.100.140, 172.17.100.148, 172.17.100.177	Security Update for Microsoft .NET Core (October 2025)	CVE-2025-55248	Medium	Open
TDL-107	192.168.10.134, 172.17.100.112	Security Update for Microsoft Visual Studio Code (November 2025)	CVE-2025-62453	Medium	Open
TDL-108	192.168.150.199, 192.168.10.20	SSL Certificate Signed Using Weak Hashing Algorithm	CVE-2005-4900	Medium	Open
TDL-109	192.168.150.199, 192.168.10.80, 192.168.10.184, 192.168.150.29, 192.168.150.139, 192.168.150.238, 192.168.150.71, 172.17.100.31, 172.17.100.32, 172.17.100.68, 172.17.100.152, 172.17.100.146, 172.17.100.147, 172.17.100.148	WinRAR < 7.11 Mark of the Web Bypass (CVE-2025-31334)	CVE-2025-31334	Medium	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
TDL-110	192.168.10.127, 172.17.100.20, 192.168.10.20, 172.17.100.53, 172.17.100.68, 172.17.100.33, 172.17.100.148, 172.17.100.177, 172.17.100.145	Curl Use-After-Free < 7.87 (CVE-2022-43552)	CVE-2022-43552	Medium	Open
TDL-111	192.168.10.127, 172.17.100.35	Microsoft OneNote Spoofing(June 2023)	CVE-2023-33140	Medium	Open
TDL-112	192.168.10.127	Security Updates for Microsoft Windows VP9 Video Extensions Library (July 2023)	CVE-2023-36872	Medium	Open
TDL-113	192.168.150.9, 192.168.150.166	Zoom Workplace < 6.5.10 Vulnerability (ZSB-25044)	CVE-2025-30669	Medium	Open
TDL-114	192.168.150.166	Node.js Module node-tar < 6.2.1 DoS	CVE-2024-28863	Medium	Open
TDL-115	172.17.100.54, 172.17.100.120	Remote Desktop Protocol Server Man-in-the-Middle Weakness	CVE-2005-1794	Medium	Open
TDL-116	172.17.100.54	Linux Distros Unpatched Vulnerability : CVE-2022-50821	CVE-2022-50821	Medium	Open
TDL-117	172.17.100.20, 172.17.100.60, 172.17.100.83	MS12-021: Vulnerability in Visual Studio Could Allow Elevation of Privilege (2651019)	CVE-2012-0008	Medium	Open
TDL-118	172.17.100.20, 172.17.100.59, 172.17.100.73, 172.17.100.83, 172.17.100.112, 172.17.100.120, 172.17.100.177	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	N/A	Medium	Open
TDL-119	172.17.100.20, 172.17.100.31, 172.17.100.32, 172.17.100.38, 172.17.100.59, 172.17.100.60,	Windows Speculative Execution Configuration Check	CVE-2022-0001	Medium	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.73, 192.168.10.20, 172.17.100.53, 172.17.100.68, 172.17.100.81, 172.17.100.83, 172.17.100.112, 172.17.100.146, 172.17.100.147, 172.17.100.33, 172.17.100.120, 172.17.100.140, 172.17.100.148, 172.17.100.141, 172.17.100.66, 172.17.100.177, 172.17.100.145				
TDL-120	172.17.100.20, 172.17.100.120, 172.17.100.140	JQuery 1.2 < 3.5.0 Multiple XSS	CVE-2020-11023	Medium	Open
TDL-121	172.17.100.20, 172.17.100.83	VMware Tools 10.x / 11.x / 12.x < 12.1.5 DoS (VMSA-2022-0029)	CVE-2022-31693	Medium	Open
TDL-122	172.17.100.31, 172.17.100.33	HTTP TRACE / TRACK Methods Allowed	CVE-2010-0386	Medium	Open
TDL-123	172.17.100.31, 172.17.100.38	Nonexistent Page (404) Physical Path Disclosure	CVE-2003-0456	Medium	Open
TDL-124	172.17.100.31	web.config File Information Disclosure	N/A	Medium	Open
TDL-125	172.17.100.32	Veeam Agent for Microsoft Windows 6.x < 6.3.2.1205 Privilege Escalation (CVE-2025-24287)	CVE-2025-24287	Medium	Open
TDL-126	172.17.100.60, 172.17.100.120	MS11-049: Vulnerability in the Microsoft XML Editor Could Allow Information Disclosure (2543893)	CVE-2011-1280	Medium	Open
TDL-127	172.17.100.60	MS11-067: Vulnerability in Microsoft Report Viewer Could Allow Information Disclosure (2578230)	CVE-2011-1976	Medium	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
TDL-128	172.17.100.60, 172.17.100.73	MS13-094: Vulnerability in Microsoft Outlook Could Allow Information Disclosure (2894514)	CVE-2013-3905	Medium	Open
TDL-129	172.17.100.60, 172.17.100.73, 172.17.100.112	MS14-024: Vulnerability in a Microsoft Common Control Could Allow Security Feature Bypass (2961033)	CVE-2014-1809	Medium	Open
TDL-130	172.17.100.60	MS15-013: Vulnerability in Microsoft Office Could Allow Security Feature Bypass (3033857)	CVE-2014-6362	Medium	Open
TDL-131	172.17.100.60, 172.17.100.73, 172.17.100.120	Security Updates for Windows 10 / Windows Server 2016 (January 2019) (Spectre)	CVE-2017-5715	Medium	Open
TDL-132	172.17.100.60, 172.17.100.73, 172.17.100.120	Windows 10 / Windows Server 2016 September 2017 Information Disclosure Vulnerability (CVE-2017-8529)	CVE-2017-8529	Medium	Open
TDL-133	172.17.100.60, 172.17.100.83	Security Updates for Windows Malicious Software Removal Tool (January 2023)	CVE-2023-21725	Medium	Open
TDL-134	172.17.100.73	Apache Tomcat Default Files	N/A	Medium	Open
TDL-135	172.17.100.73, 172.17.100.81, 172.17.100.120	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	CVE-2013-2566	Medium	Open
TDL-136	172.17.100.73, 172.17.100.112	MS13-106: Vulnerability in a Microsoft Office Shared Component Could Allow Security Feature Bypass (2905238)	CVE-2013-5057	Medium	Open
TDL-137	172.17.100.73	Security Updates for Outlook (January 2019)	CVE-2019-0559	Medium	Open
TDL-138	172.17.100.73	Security Updates for Microsoft .NET Framework (October 2020)	CVE-2020-16937	Medium	Open
TDL-139	172.17.100.73, 172.17.100.112	Security Updates for Microsoft Office Products (March 2021)	CVE-2021-27054	Medium	Open
TDL-140	172.17.100.81	SSL Weak Cipher Suites Supported	N/A	Medium	Open
TDL-141	172.17.100.81	OpenSSL AES-NI Padding Oracle MitM Information Disclosure	CVE-2016-2107	Medium	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
TDL-142	172.17.100.112, 172.17.100.177	Node.js 18.x < 18.20.6 / 20.x < 20.18.2 / 22.x < 22.13.1 / 23.x < 23.6.1 Multiple Vulnerabilities (Tuesday, January 21, 2025 Security Releases).	CVE-2025-23084	Medium	Open
TDL-143	172.17.100.33	MS13-045: Vulnerability in Windows Essentials Could Allow Information Disclosure (2813707)	CVE-2013-0096	Medium	Open
TDL-144	192.168.10.134, 192.168.150.133, 192.168.150.148, 192.168.150.180, 192.168.150.199, 192.168.10.80, 192.168.10.184, 192.168.10.194, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.115, 192.168.150.139, 192.168.150.166, 192.168.150.238, 172.17.100.35	Microsoft Windows 10 22H2 SEoL	N/A	Low	Open
TDL-145	192.168.10.127, 192.168.150.238	Windows Snip & Sketch/ Snipping Tool CVE-2023-28303 (Acropalypse)	CVE-2023-28303	Low	Open
TDL-146	172.17.100.232, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237, 172.17.100.233	OpenSSH < 10.1 / 10.1p1 Multiple Vulnerabilities	CVE-2025-61985	Low	Open
TDL-147	172.17.100.31, 172.17.100.32, 172.17.100.151, 172.17.100.146,	7-Zip < 25.01	CVE-2025-55188	Low	Open

ID	Vulnerable IP	Vulnerability Name	CVE/CWE	Severity	Status
	172.17.100.33, 172.17.100.35				
TDL-148	172.17.100.151	Microsoft Windows 11 21H2 SEoL	N/A	Low	Open
TDL-149	192.168.10.20	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	N/A	Low	Open
TDL-150	172.17.100.152	Microsoft Teams for Desktop < 25163.3611.3774.6315 Elevation of Privilege (July 2025)	CVE-2025-49731	Low	Open

Annexure A - Engagement Limitations

The security assessment was conducted within the scope and timeline agreed upon during the engagement with the Evaluated organization. Due to time limitations and operational constraints, it may not have been possible to identify every potential vulnerability present within the environment.

Testing activities were limited to the systems, endpoints, and functionalities that were made accessible by the Evaluated organization during the defined assessment period. The findings presented in this report represent the security posture of the evaluated systems at the time of testing and should not be interpreted as a guarantee that no additional vulnerabilities exist.

Annexure B - Retesting Statement

Upon completion of remediation activities by the Evaluated organization, a re-assessment may be conducted to verify whether the identified vulnerabilities have been successfully mitigated. The purpose of the re-assessment is limited to validating the remediation of the specific findings documented in this report.

The Evaluated organization is expected to address the identified vulnerabilities within a period of ninety (90) days from the date of report issuance, in accordance with the agreed remediation service level timelines. Re-assessment requests submitted within this period will be accommodated as part of the engagement to verify the implemented fixes.

Requests for re-assessment submitted after the ninety (90) day remediation window may be subject to a separate engagement or additional scope, as the validity and relevance of the original findings may change over time due to updates in the application environment.

Annexure C - Disclaimer and Precautions for Patch Implementation

Before implementing any remediation, actions based on this report, the following precautions should be observed:

- **Backup & Recovery:** Ensure complete backups of systems, applications, and data are taken prior to changes, along with a defined rollback plan to restore services in case of failure.
- **Controlled Testing:** Validate all fixes in a UAT or staging environment before deploying to production to avoid service disruption.
- **Third-Party References:** External links provided for remediation guidance are for reference only; their accuracy and availability are not guaranteed.
- **Assessment Limitations:** Findings are based on testing performed within the defined scope, timeline, and accessible environment. Certain vulnerabilities, especially those requiring intrusive testing, may not have been identified.
- **Point-in-Time Evaluation:** This report reflects the security posture at the time of assessment. New vulnerabilities may emerge due to system changes or evolving threats.
- **Ongoing Security Responsibility:** Security is a continuous process. The responsibility for implementing fixes and maintaining security controls rests with the Evaluated organization.

Annexure D - CERT-In Reporting and Remediation Compliance

As a CERT-IN empanelled organization, we have received communication stating that all CERT-IN empanelled organizations are required to submit audit-related data (including Cyber Audits, IS Audits, Regulatory audits, and VAPT audits) to CERT-IN starting from the fiscal year 2024. We will be sharing this VAPT Audit Reports or related details with CERT-IN. According to CERT-IN regulations, a period of 90 days is provided for the remediation/patching process from the release date of the audit reports. Therefore, we kindly request you to address all mentioned vulnerabilities within the 90-day timeframe and to inform us for the follow-up audit.