Analysis of Identified CVEs for DISK46 Ubuntu 24.04 Desktop Version

Date: 2025-11-13

Prepared By: Erel Rosenberg & SeongEun Kim with the support of Gemini AI

System/Scope: Ubuntu 2024.04 Desktop for Raspberry Pi including all software patches up to the report date.

Table of Contents

1. Executive Summary

This report analyzes a total of **48 Common Vulnerabilities and Exposures (CVEs)** identified in system components.

The updated vulnerability profile shows an extreme concentration of high risk: **26 CVEs are rated High or CRITICAL** (CVSS ≥ 7.0).

Primary Risk Areas:

- **Critical Integrity Compromise:** One vulnerability is rated CRITICAL (CVSS 9.4).
- **Privilege Escalation & Code Execution:** Multiple High CVEs related to Linux components (e.g., Python tarfile, X.Org, PAM, BlueZ).

Immediate Action Required: All **CRITICAL (P0)** and **HIGH (P1)** CVEs must be addressed and patched within 72 hours. All identified DoS vectors require immediate review for network-level mitigation.

2. Scope and Methodology

The risk assessment classifies vulnerabilities based on their Common Vulnerability Scoring System (CVSS) Base Score, where available. The following tiers are used:

Risk Tier	CVSS Score Range	Description	Action Priority
CRITICAL	9.0 – 10.0	**Immediate, catastrophic threat (e.g., Remote File System Overwrite).**	**P0: URGENT, Stop-the-line**
HIGH	7.0 – 8.9	Significant potential for system compromise, privilege escalation, or major service interruption.	P1: Patch within 72 hours
MEDIUM	4.0 – 6.9	Potential for limited impact or requires specific conditions to exploit.	P2: Schedule patching within 30 days
LOW	0.1 – 3.9	Minimal threat; often requires local access or user interaction.	P3: Address in next routine cycle
DoS Vector	N/A (HTTP 429)	Indicates potential for Rate Limiting Bypass or Resource Exhaustion attack.	P1/P2: Review network filtering/rate limits immediately

3. Vulnerability Profile and Detailed Analysis

3.1. CRITICAL & HIGH Severity Vulnerabilities (P0 & P1 Priority)

A total of **26 CVEs** fall into the highest risk tiers, including one CRITICAL vulnerability that mandates immediate action.

CVE ID	CVSS Score	Risk Tier	Primary Risk (Specific Component)
CVE-2025-4517	9.4	CRITICAL (P0)	**Arbitrary File Write / Extraction Bypass** (Python tarfile)
CVE-2025-11561	8.8	HIGH	**Privilege Escalation / Impersonation** (SSSD/AD Integration)
CVE-2023-44431	8.0	HIGH	**Remote Code Execution / Buffer Overflow** (BlueZ Audio Profile)
CVE-2024-9287	7.8	HIGH	**Code Execution / Privilege Escalation** (Python 3.12)
CVE-2022-33064	7.8	HIGH	**Arbitrary Code Execution** (libsndfile)
CVE-2025-7425	7.8	HIGH	**Use-After-Free / Heap Corruption** (libxslt1.1)
CVE-2025-8941	7.8	HIGH	**Privilege Escalation** (linux-pam/pam_namespace)
CVE-2024-12254	7.5	HIGH	**Denial of Service / Memory Exhaustion** (Python asyncio)
CVE-2024-6232	7.5	HIGH	**ReDoS / Denial of Service** (Python tarfile)
CVE-2024-4948	7.5	HIGH	**Denial of Service / Integer Underflow** (libsoup)
CVE-2025-12105	7.5	HIGH	**Use-After-Free / Denial of Service** (libsoup)
CVE-2025-32049	7.5	HIGH	**Denial of Service / Resource Exhaustion** (libsoup)

CVE-2025-4138	**7.5**	**HIGH**	**Extraction Filter Bypass / File Modification** (Python tarfile)
CVE-2025-4330	**7.5**	**HIGH**	**Extraction Filter Bypass / Arbitrary Write** (Python tarfile)
CVE-2025-4435	**7.5**	**HIGH**	**Extraction Filter Bypass / Arbitrary Extraction** (Python tarfile)
CVE-2025-4948	**7.5**	**HIGH**	**Denial of Service / Integer Underflow** (libsoup)
CVE-2025-52194	**7.5**	**HIGH**	**Buffer Overflow / Potential Code Execution** (libsndfile)
CVE-2025-8194	**7.5**	**HIGH**	**Infinite Loop / Denial of Service** (Python tarfile)
CVE-2022-4055	**7.4**	**HIGH**	**Integrity Compromise / Data Leakage** (xdg-utils)
CVE-2025-5024	**7.4**	**HIGH**	**Denial of Service / Resource Exhaustion** (gnome-remote-desktop)
CVE-2025-62230	**7.3**	**HIGH**	**Use-After-Free / Privilege Escalation** (X.Org X server)
CVE-2025-62231	**7.3**	**HIGH**	**Integer Overflow / Memory Corruption** (X.Org X server)
CVE-2025-31344	**7.3**	**HIGH**	**Heap Buffer Overflow / Denial of Service** (giflib)
CVE-2023-51596	**7.1**	**HIGH**	**Remote Code Execution / Heap Overflow** (BlueZ)
CVE-2023-5574	**7.0**	**HIGH**	**Use-After-Free / Privilege Escalation** (xserver-xorg-core)
CVE-2024-42040	**8.1**	**HIGH**	**Buffer Overflow / Memory Leak** (U-Boot)

3.2. Medium Severity Vulnerabilities (P2 Priority)

CVE ID	CVSS Score	CVE ID	CVSS Score	CVE ID	CVSS Score
CVE-2019-11840	5.9	CVE-2023-51594	5.7	CVE-2024-38950	6.5
CVE-2020-27748	6.5	CVE-2023-5616	4.9	CVE-2024-46421	6.8
CVE-2021-31879	6.1	CVE-2024-38949	6.5	CVE-2024-50613	6.5
CVE-2023-27043	5.3	CVE-2024-52615	5.3	CVE-2025-32907	5.3
CVE-2023-39327	4.3	CVE-2024-52616	5.3	CVE-2025-4035	4.3
CVE-2023-39328	5.5	CVE-2025-11568	4.4	CVE-2025-4476	4.3
CVE-2023-39329	6.5	CVE-2025-4969	6.5	CVE-2025-6069	4.3
CVE-2023-42366	5.5	CVE-2025-9901	5.9		
CVE-2023-51580	5.7	CVE-2023-51589	5.7	CVE-2023-51592	5.7

3.3. Denial of Service (DoS) & Low Severity Vectors

CVE ID	CVSS Score	Category	Implied Risk
CVE-2023-6873	N/A	DoS Vector	Resource Exhaustion (Thunderbird)
CVE-2024-12718	N/A	DoS Vector	Resource Exhaustion (Python 3.12)
CVE-2024-7592	N/A	DoS Vector	Resource Exhaustion (Python 3.12)
CVE-2024-8088	N/A	DoS Vector	Resource Exhaustion (Python 3.12)
CVE-2024-8383	N/A	DoS Vector	Resource Exhaustion (Python 3.12)
CVE-2024-9287	N/A	DoS Vector	Resource Exhaustion (Python 3.12)
CVE-2025-0938	N/A	DoS Vector	Parsing Differential (Python urllib)
CVE-2025-11021	N/A	DoS Vector	Resource Exhaustion (libsoup)
CVE-2025-4138	N/A	DoS Vector	Resource Exhaustion (Python 3.12)
CVE-2025-4435	N/A	DoS Vector	Resource Exhaustion (Python 3.12)
CVE-2025-4945	N/A	DoS Vector	Integer Overflow (libsoup)
CVE-2025-6141	N/A	DoS Vector	Resource Exhaustion (ncurses)
CVE-2025-62229	N/A	DoS Vector	Memory Corruption / Crash (X.Org)
CVE-2024-58251	2.5	LOW	Minimal Impact / Local
CVE-2024-7883	3.7	LOW	Minimal Impact / Local
CVE-2025-50422	2.9	LOW	Minimal Impact / Local
CVE-2025-46394	3.2	LOW	Minimal Impact / Local
CVE-2025-5918	3.9	LOW	Minimal Impact / Local

4. Priority Action Plan

The following actions are mandatory to address the heightened risks identified:

4.1. CRITICAL & Immediate Mitigation (P0 & P1)

1. **P0 CRITICAL Patching (CVE-2025-4517):** Immediately isolate systems containing vulnerable Python tarfile module and apply patches for **CVE-2025-4517 (CVSS 9.4)**. This extraction vulnerability allows remote arbitrary file writes and is the highest priority.
2. **Inventory & Patch Highs (25 CVEs):** Apply vendor patches for all 25 High Severity CVEs (CVSS 7.0+) within 72 hours, prioritizing system components dealing with authentication (SSSD), network processing (libsoup), and core Python utilities.
3. **DoS Mitigation:** Implement or review aggressive rate-limiting policies at the firewall/load balancer level to protect against the 12 specific DoS vectors identified by the HTTP 429 responses and libsoup/Python resource exhaustion flaws.

4.2. Scheduled Maintenance (P2: Medium Severity)

1. **Vulnerability Remediation:** Schedule patching for all 19 Medium Severity CVEs (CVSS 4.0 - 6.9) to be completed during the next scheduled maintenance window, targeting completion within 30 days.

4.3. Continuous Monitoring

1. **Vulnerability Scanning:** Increase the frequency of automated vulnerability scanning to ensure new CVEs associated with these components are detected immediately.
2. **Patch Verification:** Post-patching, run verified penetration tests to confirm that the critical vulnerabilities have been completely remediated.