Risk Priority List

This list prioritizes the identified vulnerabilities based on their severity and potential impact, guiding the order of remediation efforts.

1. Critical Vulnerabilities

Priority	Vulnerability ID	Description	Severity	CVSS Score	CVE Mapping	Remediation Recommendation
1	VULN-001	Outdated OpenSSH Server (8.9p1) with RCE vulnerability	Critical	9.8	CVE-2024-6387	Immediately update OpenSSH to the latest stable version. Consider restricting SSH access.

2. High Vulnerabilities

Priority	Vulnerability ID	Description	Severity	CVSS Score	CVE Mapping	Remediation Recommendation
2	VULN-002	Outdated Linux Kernel (6.1.102) with multiple security issues	High	7.8	Multiple (USN-8013-4)	Apply all pending kernel updates and reboot the system.
3	VULN-005	Missing Security Patches for various packages	High	7.5	Multiple	Regularly update all system packages and implement a patching schedule.

3. Medium Vulnerabilities

Priority	Vulnerability ID	Description	Severity	CVSS Score	CVE Mapping	Remediation Recommendation
4	VULN-004	Weak SSH Configuration	Medium	4.3	N/A	Review and harden SSH configuration based on security best practices.
5	VULN-003	VNC Authentication Enabled (potential for weak authentication)	Medium	5.3	CVE-2006-2369 (Potential)	Identify VNC server version, upgrade if outdated, use strong passwords, consider SSH tunneling, and restrict access.