**CVE Vulnerability Report**

**Image**: dmesa2/sa\_assessment  
**Base OS**: Ubuntu 22.04  
**Date of Scan**: October 7, 2024

**Vulnerabilities Summary**

| **Severity** | **CVE ID** | **Package** | **Version** | **Score** | **Fixed in** |
| --- | --- | --- | --- | --- | --- |
| Medium | CVE-2022-0391 | python2.7 | 2.7.18-13ubuntu1.2 | 7.5 | - |
| Medium | CVE-2023-24329 | python2.7 | 2.7.18-13ubuntu1.2 | 7.5 | - |
| Medium | CVE-2021-4189 | python2.7 | 2.7.18-13ubuntu1.2 | 5.3 | - |
| Medium | CVE-2023-27043 | python2.7 | 2.7.18-13ubuntu1.2 | 5.3 | - |
| Medium | CVE-2023-4039 | gcc-12 | 12.3.0-1ubuntu1~22.04 | 4.8 | - |
| Medium | CVE-2024-2236 | libgcrypt20 | 1.9.4-3ubuntu3 | - | - |
| Medium | CVE-2024-26462 | krb5 | 1.19.2-2ubuntu0.4 | - | - |
| Low | CVE-2016-20013 | glibc | 2.35-0ubuntu3.8 | 7.5 | - |
| Low | CVE-2017-11164 | pcre3 | 2:8.39-13ubuntu0.22.04.1 | 7.5 | - |
| Low | CVE-2019-17514 | python2.7 | 2.7.18-13ubuntu1.2 | 7.5 | - |
| Low | CVE-2019-9674 | python2.7 | 2.7.18-13ubuntu1.2 | 7.5 | - |
| Low | CVE-2022-41409 | pcre2 | 10.39-3ubuntu0.1 | 7.5 | - |
| Low | CVE-2022-4899 | libzstd | 1.4.8+dfsg-3build1 | 7.5 | - |
| Low | CVE-2024-7592 | python2.7 | 2.7.18-13ubuntu1.2 | 7.5 | - |
| Low | CVE-2016-2781 | coreutils | 8.32-4.1ubuntu1.2 | 6.5 | - |
| Low | CVE-2023-50495 | ncurses | 6.3-2ubuntu0.1 | 6.5 | - |
| Low | CVE-2023-7008 | systemd | 249.11-0ubuntu3.12 | 5.9 | - |
| Low | CVE-2022-27943 | gcc-12 | 12.3.0-1ubuntu1~22.04 | 5.5 | - |
| Low | CVE-2022-3219 | gnupg2 | 2.2.27-3ubuntu2.1 | 3.3 | - |
| Low | CVE-2023-29383 | shadow | 1:4.8.1-2ubuntu2.2 | 3.3 | - |
| Low | CVE-2023-45918 | ncurses | 6.3-2ubuntu0.1 | - | - |
| Low | CVE-2024-26458 | krb5 | 1.19.2-2ubuntu0.4 | - | - |
| Low | CVE-2024-26461 | krb5 | 1.19.2-2ubuntu0.4 | - | - |
| Low | CVE-2024-41996 | openssl | 3.0.2-0ubuntu1.18 | - | - |

**Recommendations**

1. **Upgrade Packages:**
   * We should consider upgrading to a newer version of Python or switching to Python 3 if possible, as Python 2 has reached end-of-life.
   * We need to review each package to determine if newer versions are available that address the reported vulnerabilities.
   * We should look at upgrading base Ubuntu image from 22.04 to 24.04.
2. **Monitor and Patch:**
   * We should regularly monitor our image for new vulnerabilities and patch them promptly.
   * We should set up automatic vulnerability scanning to alert us to newly identified issues.
3. **Evaluate Dependencies:**
   * We should evaluate the need for specific packages that are known to have vulnerabilities, especially those with medium or high severity scores.
4. **Use Docker Best Practices:**
   * We should consider using multi-stage builds to minimize the final image size and surface area for vulnerabilities.

**Conclusion**

Regular vulnerability scanning and timely updates are crucial in maintaining the security of our application. We need to ensure we have a process in place for continuous security assessment and management.