## RMF Report for Operating System Patch Management

Date: 03-11-2025

Time: 08:57:55

OS Name: RMF-Client01

OS Version: #1 SMP PREEMPT\_DYNAMIC Debian 6.1.128-1 (2025-02-07)

Computer Name: RMF-Client01

IP Address: 10.0.0.20

CVE List for Unpatched Programs:

1. firefox-esr

Current version: 128.7.0esr-1~deb12u1

Update version: 128.8.0esr-1~deb12u1

Affiliated CVES:

CVE-2009-3377

CVE-2012-5842

CVE-2023-4057

2. fonts-opensymbol

Current version: 4:102.12+LibO7.4.7-1+deb12u6

Update version: 4:102.12+LibO7.4.7-1+deb12u7

Affiliated CVES:

CVE-2021-25635

3. libreoffice-base-core

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

4. libreoffice-calc

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

5. libreoffice-common

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

6. libreoffice-core

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

7. libreoffice-draw

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

8. libreoffice-gnome

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

9. libreoffice-gtk3

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

10. libreoffice-help-common

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

11. libreoffice-help-en-us

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

12. libreoffice-impress

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

13. libreoffice-math

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

14. libreoffice-style-colibre

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

15. libreoffice-style-elementary

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

16. libreoffice-writer

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

17. libuno-cppu3

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

18. libuno-cppuhelpergcc3-3

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

19. libuno-purpenvhelpergcc3-3

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

20. libuno-sal3

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

21. libuno-salhelpergcc3-3

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

22. python3-uno

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

23. uno-libs-private

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

24. ure

Current version: 4:7.4.7-1+deb12u6

Update version: 4:7.4.7-1+deb12u7

Affiliated CVES:

CVE-2015-0835

CVE-2021-41832

25. xserver-common

Current version: 2:21.1.7-3+deb12u8

Update version: 2:21.1.7-3+deb12u9

Affiliated CVES:

None

26. xserver-xephyr

Current version: 2:21.1.7-3+deb12u8

Update version: 2:21.1.7-3+deb12u9

Affiliated CVES:

None

27. xserver-xorg-core

Current version: 2:21.1.7-3+deb12u8

Update version: 2:21.1.7-3+deb12u9

Affiliated CVES:

None

28. xserver-xorg-legacy

Current version: 2:21.1.7-3+deb12u8

Update version: 2:21.1.7-3+deb12u9

Affiliated CVES:

None

Patch Deployment:

Apply all pending updates immediately to prevent potential security risks and disruptions.

Operational Problems:

Before applying the patches, ensure that your system is backed up and take necessary measures to minimize operational disruption. Additionally, consider running a thorough test environment before deploying the patches to any production systems.