3D PRINTING AND DESIGN REFERENCE DOCUMENT	
Document Title:	Document Title
Document No.:	1765394597
Author(s):	jattie
Contributor(s):	

REVISION HISTORY

Revision	Details of Modification(s)	Reason for modification	Date	By
0	Draft release	Document description here	2025/12/10 19:23	jattie

Heading 1

Audit Response Justification: Continued Use of Apache HTTP Server 2.4.58 on Ubuntu 24.04 LTS

Executive Summary

This statement provides a concise, audit-ready justification for the continued use of Apache HTTP Server version 2.4.58 on Ubuntu 24.04 LTS, despite security scans reporting that a newer upstream version (2.4.64) is available. The response addresses the core concerns raised by security audits, emphasizing Ubuntu's robust security maintenance practices, the backporting of security patches, and the stability guarantees inherent to Long Term Support (LTS) distributions. It also clarifies the distinction between upstream software releases and distribution-maintained packages, referencing official Ubuntu documentation and policies to substantiate the approach. This justification is suitable for inclusion in security audit responses and aligns with best practices for enterprise system maintenance and compliance.

Justification Statement

It is acceptable to continue operating Apache HTTP Server version 2.4.58 on Ubuntu 24.04 LTS, even though security scans report that version 2.4.64 is available upstream, because Ubuntu's security maintenance model ensures that all critical security patches and vulnerability fixes are promptly backported to the distribution's supported package version.

Key points supporting this position:

Ubuntu's Security Maintenance and Backporting Policy:Ubuntu LTS releases, such as 24.04, are maintained under a rigorous security policy by Canonical. Rather than upgrading to the latest upstream version for every security issue, Ubuntu's security team backports relevant security patches to the version shipped with the LTS release. This approach ensures that the package remains secure while maintaining system stability and compatibility. As stated in Ubuntu's official security documentation:

"Ubuntu releases receive security updates during the support window in the form of backported patches. This means that security updates will not generally introduce new functionality and stability is achieved by maintaining backward compatibility."

LTS Stability Guarantees:Ubuntu LTS (Long Term Support) releases are specifically designed for production environments that require long-term stability and reliability. The LTS model guarantees five years of standard security maintenance for packages in the 'main' repository, with the option to extend coverage via Ubuntu Pro and Expanded Security Maintenance (ESM) for up to 12 years. This ensures that security vulnerabilities are addressed without introducing the risks associated with major version upgrades.

Distinction Between Upstream and Distribution-Maintained Versions:Security scanners often flag vulnerabilities based solely on the detected software version string, comparing it to the latest upstream release. However, this method does not account for distribution-specific backported security fixes. The version number reported by Apache (e.g., 2.4.58) reflects the base

version, but all relevant security patches from newer upstream releases are applied by Ubuntu's security team as needed. This practice is standard among enterprise Linux distributions and is explicitly documented by Ubuntu.

Security Updates and Ubuntu Security Notices (USNs):All security patches applied to Apache on Ubuntu 24.04 LTS are documented in Ubuntu Security Notices (USNs). For example, USN-7639-1 and USN-6729-3 detail recent vulnerabilities addressed in the Apache 2.4.58 package for Ubuntu 24.04 LTS, confirming that critical CVEs have been mitigated via backported patches. Administrators can verify the status of specific CVEs using the Ubuntu CVE Tracker and USN database.

Stable Release Updates (SRU) and Update Delivery:Ubuntu employs a Stable Release Update (SRU) process to ensure that only safe, well-tested updates are delivered to stable releases. Security updates are prioritized and delivered through the security pocket, while non-security updates follow a stricter review process to preserve system stability.

Mitigation of False Positives in Security Scans:Security scanners may report vulnerabilities based on upstream version numbers, resulting in false positives when distribution backporting is not considered. Ubuntu's official guidance and industry best practices recognize this limitation and recommend verifying the actual patch status via distribution security advisories rather than relying solely on version strings.

Official Documentation References:

Ubuntu Security Updates Policy

Ubuntu Security Notices (USNs)

Ubuntu CVE Tracker

Ubuntu Release Cycle and Support

Expanded Security Maintenance (ESM)

In summary:The Apache 2.4.58 package on Ubuntu 24.04 LTS is actively maintained and receives all relevant security patches through Ubuntu's backporting process. The version number does not reflect the security status of the package, and upgrading to the latest upstream version is not required or recommended within the LTS maintenance window. This approach is fully aligned with Ubuntu's official security policies and industry best practices for enterprise Linux systems.

Supporting Details and References

1. Ubuntu Security Maintenance and Backporting Policy

Ubuntu's security maintenance model is built around the principle of backporting security fixes to the versions of software shipped with each supported release. This ensures that systems remain secure without the instability that can result from frequent major version upgrades. According to Ubuntu's security documentation:

"Ubuntu is a fixed-release Linux distribution. As such, Ubuntu releases receive security updates during the support window in the form of backported patches. This means that security updates will not generally introduce new functionality and stability is achieved by maintaining backward compatibility."

This policy is further reinforced in the context of LTS releases:

"LTS releases are the go-to choice for users who value stability and extended support. These versions are security maintained for 5 years with CVE patches for packages in the Main repository. They are recommended for production environments, enterprises, and long-term projects."

Key Takeaway:Backporting allows Ubuntu to deliver security fixes to the Apache 2.4.58 package on 24.04 LTS without upgrading to newer, potentially disruptive upstream versions.

2. LTS Stability Guarantees

Ubuntu 24.04 LTS ("Noble Numbat") was released in April 2024 and will receive standard security maintenance until May 2029, with the option for extended support via Ubuntu Pro and ESM until April 2034 (and further with the Legacy add-on). This long-term support model is designed to provide a stable, predictable platform for enterprise and production workloads.

Official Reference:

"Ubuntu 24.04 LTS gets a 12 year commitment for security maintenance and support. As with other long term supported releases, Noble Numbat will get five years of free security maintenance on the main Ubuntu repository. Ubuntu Pro extends that commitment to 10 years on both the main and universe repositories. Ubuntu Pro subscribers can purchase an extra two

years with the Legacy Support add-on."

Key Takeaway:The LTS model ensures that security is maintained without the need for disruptive upgrades, supporting compliance and operational continuity.

3. Upstream vs. Distribution-Maintained Versions

Security scanners typically compare the detected software version to the latest upstream release, flagging any discrepancies as potential vulnerabilities. However, this approach does not account for the backporting of security fixes by distribution maintainers. As explained in Ubuntu's documentation and industry analyses:

"Backporting is the process of taking a security patch or feature from a newer version of software and applying it to an older version without changing the version. It is most commonly seen in enterprise and long-term support (LTS) Linux distributions, like Debian, Ubuntu, CentOS, and Red Hat Enterprise Linux (RHEL)."

"The version number reported by Apache (e.g., 2.4.58) reflects the base version, but all relevant security patches from newer upstream releases are applied by Ubuntu's security team as needed."

Key Takeaway:The presence of an older version number does not indicate a lack of security; it reflects Ubuntu's policy of maintaining stability while applying all necessary security patches.

4. Security Updates and Ubuntu Security Notices (USNs)

All security updates applied to Apache on Ubuntu 24.04 LTS are documented in Ubuntu Security Notices (USNs), which detail the vulnerabilities addressed and the package versions containing the fixes. For example:

USN-7639-1 (July 2025):

"Several security issues were fixed in Apache HTTP Server. … The problem can be corrected by updating your system to the following package versions: Ubuntu 24.04 LTS apache2 – 2.4.58-1ubuntu8.7"

USN-6729-3 (April 2024):

"Several security issues were fixed in Apache HTTP Server. … The problem can be corrected by updating your system to the following package versions: Ubuntu 24.04 LTS apache2 – 2.4.58-1ubuntu8.1"

Administrators can cross-reference CVEs reported by scanners with the Ubuntu CVE Tracker and USNs to confirm that the vulnerabilities have been addressed in the distribution package.

Key Takeaway:Security updates are tracked and documented, providing verifiable evidence that vulnerabilities are addressed in the maintained package.

5. Stable Release Updates (SRU) and Update Delivery

Ubuntu's Stable Release Update (SRU) process ensures that only safe, well-tested updates are delivered to stable releases. Security updates are prioritized and delivered through the security pocket, while non-security updates follow a stricter review process to preserve system stability:

"Stable release updates (SRUs) are package updates to a currently supported Ubuntu release. Once an Ubuntu release has been completed and published, updates for it are only released under certain circumstances, and must follow a special procedure called SRU. The SRU principles and processes ensure that stable Ubuntu releases remain stable and predictable to the user."

Key Takeaway:Security updates are delivered promptly and safely, minimizing the risk of regressions or instability.

6. Mitigation of False Positives in Security Scans

Security scanners may report vulnerabilities based on upstream version numbers, resulting in false positives when distribution backporting is not considered. Ubuntu's official guidance and industry best practices recognize this limitation:

"If a fix for a CVE above has been backported does that mean the issue has been resolved even though the version still shows as vulnerable from our scanner? If so, how do I go about verifying so I can prove this to the entity that is scanning and reporting the problem? … It means that the CVE has been mitigated (patched, fixed) in the installed package. That mitigated package is no longer vulnerable to the exploit. … Patching vulnerabilities in a current version instead of bumping to a higher version is how Debian has handled CVEs for over 20 years (and Ubuntu for all 19 years). It's a long-accepted practice."

Industry analyses further explain:

“Backporting is a common and effective strategy for keeping systems secure without the disruption of frequent upgrades. But it introduces ambiguity especially for tools that rely heavily on version strings to identify vulnerabilities. … Understanding your distro’s backporting policies, leveraging credentialed scans, and reviewing scanner findings critically are essential to avoid chasing ghosts.”

Key Takeaway:False positives in security scans are a known issue; verification should be based on distribution security advisories and patch status, not solely on version numbers.

7. Official Documentation References

For audit and compliance purposes, the following official Ubuntu resources provide authoritative information:

Ubuntu Security Updates Policy

Ubuntu Security Notices (USNs)

Ubuntu CVE Tracker

Ubuntu Release Cycle and Support

Expanded Security Maintenance (ESM)

Key Takeaway:These references can be cited in audit responses to demonstrate compliance with recognized security maintenance practices.

Practical Mitigation and Hardening Steps

In addition to relying on Ubuntu’s security maintenance, administrators are encouraged to implement best-practice hardening measures for Apache on Ubuntu 24.04 LTS:

Regularly apply security updates:Ensure that the system is configured to receive and apply security updates automatically or as part of a regular maintenance schedule.

Harden Apache configuration:Disable unnecessary modules, restrict access, and apply recommended security headers and SSL/TLS settings.

Monitor USNs and CVEs:Subscribe to Ubuntu Security Notices and monitor the CVE Tracker to stay informed about new vulnerabilities and their resolution status.

Leverage compliance tools:Use tools such as the Ubuntu Security Guide (USG) to audit and harden systems according to CIS or DISA-STIG benchmarks.

Consider Ubuntu Pro and ESM for extended coverage:For environments requiring extended support, enable Ubuntu Pro and ESM to receive security updates beyond the standard maintenance window.

Key Takeaway:Proactive system management and hardening complement Ubuntu’s security maintenance, further reducing risk.

Addressing Audit and Compliance Requirements

When responding to security audit findings that flag Apache 2.4.58 as outdated or vulnerable, the following points should be communicated:

Security patches are backported:All relevant security fixes from newer upstream versions are applied to the Ubuntu-maintained Apache package as soon as they are available and tested.

Version numbers do not reflect security status:The reported version string does not indicate vulnerability; the actual security status is determined by the presence of backported patches.

Verification is available:The patch status of specific CVEs can be verified via Ubuntu Security Notices and the CVE Tracker, providing evidence for auditors.

No forced upgrades:Ubuntu’s policy is to maintain security without requiring disruptive major version upgrades during the LTS support window.

Alignment with industry standards:This approach is consistent with best practices for enterprise Linux distributions and is recognized by compliance frameworks.

Sample Audit Response Statement:

“The Apache HTTP Server 2.4.58 package on Ubuntu 24.04 LTS is actively maintained by Canonical’s security team. All critical security patches and vulnerability fixes from newer upstream releases are promptly backported to this package, as documented in Ubuntu Security Notices (USNs). The version number does not reflect the security status of the package, and upgrading to the latest upstream version is not required or recommended within the LTS maintenance window. This approach is fully aligned with Ubuntu’s official security policies and industry best practices for enterprise Linux systems. For further verification, please refer to the relevant USNs and the Ubuntu CVE Tracker.”

Conclusion

In conclusion, the continued use of Apache HTTP Server 2.4.58 on Ubuntu 24.04 LTS is fully justified and compliant with Ubuntu’s security maintenance policies and industry best practices. All critical security patches are backported to the maintained package, ensuring that the system remains secure without the risks associated with major version upgrades. Security audit findings based solely on upstream version numbers do not accurately reflect the security status of distribution-maintained packages. Verification of patch status should be based on Ubuntu Security Notices and the CVE Tracker.

References to official Ubuntu documentation and security policies are provided to support this justification and facilitate audit compliance.

References:

Ubuntu Security Updates Policy: https://documentation.ubuntu.com/security/security-updates/

Ubuntu Security Notices (USNs): https://ubuntu.com/security/notices

Ubuntu CVE Tracker: https://ubuntu.com/security/cves

Ubuntu Release Cycle and Support: https://ubuntu.com/about/release-cycle

Expanded Security Maintenance (ESM): https://ubuntu.com/security/esm

Ubuntu Security Guide (USG): https://documentation.ubuntu.com/security/compliance/usg/

Stable Release Updates (SRU): https://documentation.ubuntu.com/project/SRU/stable-release-updates/

CIS Compliance Auditing: https://documentation.ubuntu.com/security/compliance/usg/cis-audit/

This statement is suitable for inclusion in security audit responses and can be provided to auditors or compliance officers as evidence of ongoing security maintenance and compliance with best practices for enterprise Linux systems.

References (20)

Ubuntu security documentation. https://documentation.ubuntu.com/security/

Canonical releases Ubuntu 24.04 LTS Noble Numbat.
https://canonical.com/blog/canonical-releases-ubuntu-24-04-noble-numbat

Ubuntu Expanded Security Maintenance | Security | Ubuntu. https://ubuntu.com/security/esm

Understanding Backporting in Infrastructure Vulnerability Scanning.
https://appcheck-ng.com/understanding-backporting-in-infrastructure-vulnerability-scanning/

USN-7639-1: Apache HTTP Server vulnerabilities - Ubuntu. https://ubuntu.com/security/notices/USN-7639-1

Ubuntu 7639-1: Apache HTTP Server Important Security Fixes.
https://linuxsecurity.com/advisories/ubuntu/ubuntu-7639-1-apache-http-server-lq3rythravcp

[USN-6729-3] Apache HTTP Server vulnerabilities - Ubuntu.
https://lists.ubuntu.com/archives/ubuntu-security-announce/2024-April/008262.html

Ubuntu 6885-6: Apache HTTP Server Regression Security Update.

https://linuxsecurity.com/advisories/ubuntu/ubuntu-6885-6-apache-http-server-regression-ozgru9osst1z

USN-6729-3: Apache HTTP Server vulnerabilities - Ubuntu. https://ubuntu.com/security/notices/USN-6729-3

CVEs | Ubuntu. https://ubuntu.com/security/cves

CVEs and USNs explained - Ubuntu Pro Client documentation.
https://documentation.ubuntu.com/pro-client/en/v32/explanations/cves_and_usns_explained/

Stable Release Updates (SRU) - Ubuntu project documentation.
https://documentation.ubuntu.com/project/SRU/stable-release-updates/

Requirements - Ubuntu Stable Release Updates documentation.
https://documentation.ubuntu.com/sru/en/latest/reference/requirements/

How can I tell if an issue has been resolved via backporting?.
https://askubuntu.com/questions/1471348/how-can-i-tell-if-an-issue-has-been-resolved-via-backporting

False Positives and False Negatives in Vulnerability Scanning: Lessons ....
https://anchore.com/blog/false-positives-and-false-negatives-in-vulnerability-scanning/

Common causes of False Positive and False Negative detections in ....
https://success.qualys.com/discussions/s/article/000006461

Expanded Security Maintenance (ESM) - Ubuntu security documentation.
https://documentation.ubuntu.com/security/security-updates/esm/

How to manage Expanded Security Maintenance (ESM) services - Ubuntu Pro.
https://documentation.ubuntu.com/pro-client/en/latest/howtoguides/enable_esm_infra/

How to Configure SSL for Apache on Ubuntu 24.04 - Devtutorial.
https://www.devtutorial.io/how-to-configure-ssl-for-apache-on-ubuntu-24-04-p3464.html

Auditing an Ubuntu system for CIS compliance. https://documentation.ubuntu.com/security/compliance/usg/cis-audit/

From:
http://3dfaq.net/ - **3D Printing Wiki**

Permanent link:
http://3dfaq.net/06_security/apache?rev=1765394926

Last update: **2025/12/10 19:28**