Red Hat backporting FAQ

- Explanation:

  https://access.redhat.com/security/updates/backporting

- More info below (from https://access.redhat.com/solutions/57665)

What is backporting and how does it affect Red Hat Enterprise Linux (RHEL)?

Issue

- What is backporting and how does it affect Red Hat Enterprise Linux (RHEL)?
- The recommended RHEL package version for a CVE does not match the upstream package version.
- Why are RHEL package versions behind the upstream versions?

Resolution

Backporting security fixes

- Red Hat use the term backporting to describe when it take a fix for a security flaw out of the most recent version of an upstream software package, and apply that fix to an older version of the package Red Hat distributed.
- Backporting will be a new concept for those more familiar with proprietary software updates. Here is an example of why Red Hat backport security fixes:
- Red Hat shipped version 2.0.40 of the Apache HTTP Server with Red Hat Linux 8.0. Shortly after the release, a number of security issues were found and disclosed by the Apache Software Foundation. The Apache Software Foundation issued a new release, Apache HTTP Server 2.0.43, which contained fixes for those issues; however, in addition to the security fixes, a number of other changes (bug fixes and new features) were made between versions 2.0.40 and 2.0.43.
- One of these features changed the module interface. In this case, if Red Hat issued a security update with version 2.0.43 of the Apache HTTP Server, replacing version 2.0.40, any modules which were in use would need be updated (recompiled) to match the new module interface. If third-party modules are being used, needs to go to the supplier of those modules to get updates. Moving from version 2.0.40 to 2.0.43 of the Apache HTTP Server would require manual effort by system administrators. Such an update would not be suitable for automated upgrade systems such as the Red Hat Network.
- In cases like these Red Hat can backport the updates. When Red Hat backport security fixes Red Hat:
  - identify the fixes and isolate them from any other changes.
  - make sure the fixes do not introduce unwanted side effects.
  - apply the fixes to previously released versions.
- For most products the default practice is to backport security fixes, but Red Hat do sometimes provide version updates for some packages after careful testing and analysis. These are likely to be packages that have no interaction with others, or those used by an end-user, such as web browsers and instant messaging clients.

Explaining common release numbering confusion

- Backporting has a number of advantages, but it can create confusion when it is not understood. For example, stories in the press may include phrases such as "upgrade to Apache httpd 2.0.43 to fix the issue", which only takes into account the upstream version number. This can cause confusion as even after installing updated packages from a vendor, it is not likely to have the latest upstream version, but rather have an older upstream version with backported patches applied.
- Also, some security scanning and auditing tools make decisions about vulnerabilities based solely on the version number of components they find. This results in false positives as the tools do not take into account backported security fixes.
- Security issues flagged by Nessus reveals false positives
- Since the introduction of Red Hat Enterprise Linux, Red Hat has been careful to explain in it's security advisories how it fixed an issue: by moving to a new upstream version, or by backporting patches to the existing version. Red Hat has attached CVE namesto all it's advisories since January 2000, allowing all to easily cross-reference vulnerabilities and find out how and when Red Hat fixed them, independent of version numbers.
- Red Hat also supply OVAL definitions (machine-readable versions of advisories) that third-party vulnerability tools can use to determine the status of vulnerabilities, even when security fixes have been backported.
- For latest update refer: Backporting Security Fixes
- After an upstream project has released a newer version of a package when will the package on a Red Hat Enterprise Linux System be updated to this version?