The SafeRepo Initiative

Many third party repositories exist for Enterprise Linux distributions. These repositories provide several different types of packages. Not all repositories clearly describe the types of packages that are provided, which may lead to unexpected results. The SafeRepo Initiative is a set of guidelines for third part repositories to follow in order to help users avoid these unexpected results.

Terminology

- **stock distribution**: A Linux distribution as it comes from the vendor. Examples include Red Hat Enterprise Linux, CentOS, or Fedora.
- **stock package**: A package that a stock distribution provides by default in their enabled repositories.
- **third party repository**: A package repository intended for use with a Linux distribution that is not associated with the vendor of the distribution.
- **third party package**: A package that a third party repository provides.

Current Problem With Third Party Repositories

When you subscribe to third party repositories, you often don't know what will happen. Different third party repositories behave differently. Some repositories only provide additional packages that are not in the stock distribution. Other repositories contain newer versions of stock packages with the same name. Many do not fully describe they types of packages they provide, which can lead to unexpected results for end users.

When a repository doesn't clearly describe the types of packages they provide, users of the repositories are put at risk.

Here is a common example. A user subscribes to a third party repository for a newer major version of MySQL. Later, they discover that their application is broken because PHP was also updated to a new major version during updates.

Examples of Safe Repositories

- EPEL (https://fedoraproject.org/wiki/EPEL): Extra Packages for Enterprise Linux is a Fedora Special Interest Group that provides high quality additional packages for Enterprise Linux. They have strict guidelines that their packages should never conflict (https://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html#RPM_Guide-Dependencies-conflicts) with or replace packages in the base Enterprise Linux distribution. Therefore, subscribing to EPEL is safe in that nothing will happen unless you explicitly install a package from the repo.
- IUS (https://iuscommunity.org): The IUS Project provides packages for Enterprise Linux that follow

the latest upstream stable versions of specific software. IUS is a safe repository because it uses alternate package names that provide (https://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html#RPM_Guide-Dependencies-capabilities) the corresponding stock package name, but do not obsolete (https://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html#RPM_Guide-Dependencies-obsoletes) the stock package. IUS packages also explicitly conflict (https://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html#RPM_Guide-Dependencies-conflicts) with their stock counterparts to further prevent anything from IUS automatically replacing a stock package.

Examples of Unsafe Repositories

We are not going to explicitly call out specific projects, but their are ways to recognize unsafe repositories.

- Packages that obsolete (https://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html#RPM_Guide-Dependencies-conflicts) stock packages.
- Packages that use the same name as stock packages, which effectively obsoletes the stock package.

Safe Package Types

Add-on Package

- A package that provides software that does not exist in the stock distribution.
- Must not have the same name as any stock distribution package.
- Must not obsolete (https://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html#RPM_Guide-Dependencies-obsoletes) any stock distribution package.
- Must not conflict (https://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html#RPM_Guide-Dependencies-conflicts) with any stock distribution package.
- If later added to the stock distribution, it must be removed from the third party repository.

Parallel Installable Package

- A package that provides an alternate version of a stock distribution package.
- Uses a different name than the stock distribution package so it can be installed at the same time as the stock distribution package.
- Files from the package must use different names than files from stock distribution packages to avoid file conflicts.
- Must not provide (https://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html#RPM_Guide-Dependencies-capabilities) the stock distribution package name.
- Must not obsolete (https://docs.fedoraproject.org/en-

US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html#RPM_Guide-Dependencies-obsoletes) any stock distribution package.
- Must not conflict (https://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html#RPM_Guide-Dependencies-conflicts) with any stock distribution package.

Safe Replacement Package

- A package that provides an alternate version of a stock distribution package.
- Uses a different name than the stock distribution package to prevent unintended upgrades.
- Provide (https://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html#RPM_Guide-Dependencies-capabilities) the stock distribution package name to satisfy the dependencies of other packages.
- Be compatible with other stock distribution packages that depend on the stock distribution package being replaced.
- Conflict (https://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html#RPM_Guide-Dependencies-conflicts) with the stock distribution package that is being replaced.
- Replaces the functionality of the stock distribution package that is being replaced.
- Must not obsolete (https://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html#RPM_Guide-Dependencies-obsoletes) the stock distribution package that is being replaced.

Unsafe Package Types

Direct Replacement Package

- A package that provides an alternate version of a stock distribution package.
- Uses the same name as the stock distribution package to allow for direct upgrades.
- Replaces the functionality of the stock distribution package that is being replaced.
- If a repository provides this type of package, it is recommended that the repositories be disabled by default to avoid unintended upgrades.