SCF Department Patching Policy

All servers managed by the Scientific Computing Facilities Department run operating systems derived from Red Hat Enterprise Linux: either Scientific Linux or AlmaLinux. Software updates are released regularly by Red Hat, and soon after by each distribution.

Constraints

SCF tracks, and patches, only software from standard upstream repositories installed via the 'root' user:

- AlmaLinux or Scientific Linux
- Fermilab additions to SL and AlmaLinux
- EPEL
- ELRepo
- OSG
- A few approved others: HTCondor, etc.

If a customer or service owner requires any additional software that must be installed as root, and that software cannot be enabled for automatic updates, they are responsible for tracking security issues and requesting updates as needed.

In addition, if a customer or service owner requires that a standard package be frozen for any reason, they are responsible for tracking security issues for that package and requesting an update when appropriate.

Schedule

Updates that do not require rebooting the system are applied nightly. Many systems use a repository with a 30-day delay, so that patches are applied about 30 days after release. Critical updates are applied immediately.

Updates that require rebooting (typically a new version of the Linux kernel) are deferred until the next monthly maintenance window, or some other date agreed upon by SCF, service providers, and users (except for Cyber Security declared critical updates, which are applied immediately). Unless there is an approved variance for a longer interval, the time between release of a patched version and applying it (including rebooting) is not more than 60 days.

Some groups of systems, for example dCache or HPC systems, have approved variances to patch at longer intervals, typically 90 or 180 days. In those cases, patching follows the schedule specified by the variance.

Last update: February 21, 2023