Fedora Repository 3.4.1 Release Notes

About This Release

Release Date: October 19th, 2010

This bugfix release FCREPO-798, a “Denial of Service” (DOS) vulnerability affecting all prior versions of Fedora 2.x and 3.x, and FCREPO-790, a bug that could lead to the operating system running out of file handles.

FCREPO-798 was discovered during a code review and verified in testing. However, there have been no known attacks on any public or private Fedora repository. Our review indicates this vulnerability can corrupt the Fedora database in a way that will cause failure of your operating repository. However, **it cannot be used to damage your archival storage**. Fortunately, the repository may be recovered through the use of the rebuilder utility but until your system is patched it could be subject to additional DOS attacks.

A set of patches for Fedora 3.3 and Fedora 3.4 as well as a full release of Fedora 3.4.1 in which the issue is fixed has been posted on SourceForge. We ask you contact your repository operator immediately about the issue. If you are using Fedora 3.0 through 3.2, we urge you to update to patched copies of Fedora 3.3 or 3.4, or the 3.4.1 release at your earliest opportunity. The security releases may be found at:

- http://sourceforge.net/projects/fedora-commons/files/fedora/3.3.1/
- http://sourceforge.net/projects/fedora-commons/files/fedora/3.4.1/

The instructions for installation may be found in the README files at the above locations along with the downloads.

Unfortunately, Fedora 2 repositories remain vulnerable; a patch to Fedora 2, whose code base was declared at “end-of-life” two years ago, has proven beyond our resources at this time. Because of this, we will not being providing details about potential exploits in the near term. Fedora 2 installations are still of great concern to the Fedora committers since we know there are many installations in our community who may not be in a position to update to the latest Fedora release. We are seeking resources or volunteers to fix Fedora 2 but, at this time, we are not able to commit to a timeline for this work.

If you cannot update soon please read the following section containing suggestions that may help mitigate the vulnerability of your repository. Your installation may have minimal risk if Fedora is not directly exposed to un-trusted users. You should:

- Restrict access to Field Search including for front applications which pass unmodified query parameter text directly from users
- Restrict access from anonymous users for:
    - API-A Lite “get” operations
    - REST API “get” operations
    - REST API “findObjects” operations
- Restrict ingest of new digital objects from un-trusted users

If you have front-end applications (like Islandora or Muradora) which control access, the format of queries, or FOXML ingest or modifications your risks are mitigated. It is best if direct access to Fedora is hidden from users and only your front-end applications are exposed. In all cases, we recommend close monitoring of your repository.

This notification is to warn operators of production Fedora repositories. Please notify us if you have a sudden, unexplained failure of your system. As with all software, security issues may arise. We are collecting contact information for a responsible person for each production Fedora systems to help the notification process. Could you or your repository administrator please provide us with a suitable contact? If you know of any other production Fedora repositories, could you provide a suitable contact for it?

If you have any questions or are operating a Fedora system in production please contact ddavis at duraspace dot org or cwilper at duraspace dot org.

Previous Release Notes

All release notes for Fedora 3.4.x can be found here.