DSpace Release 3.4 Notes

Version 3.4

DSpace 3.4 was officially released to the public on February 24, 2015.

DSpace 3.4 can be downloaded immediately from:

- https://github.com/DSpace/DSpace/releases/tag/dspace-3.4

More information on the 3.4 release (and the 3.x platform in general) can be found in the 3.x Documentation Preface.

We highly recommend any users of DSpace 3.x (or below) upgrade to 3.4

DSpace 3.4 contains security fixes for both the XMLUI and JSPUI. To ensure your 3.x site is secure, **we highly recommend all DSpace 3.x users upgrade to DSpace 3.4**.

We also highly recommend removing any "allowLinking=true" settings from your Tomcat's <Context> configuration. Previously our installation documentation erroneously listed examples which included "allowLinking=true", while the Tomcat documentation lists it as a possible security concern. The XMLUI Directory Traversal Vulnerability (see below) is also exacerbated by this setting.

We highly recommend DSpace 1.x.x users upgrade to DSpace 3.4, 4.3 or 5.1

If you are running an older, unsupported version of DSpace (1.x.x), we highly recommend upgrading to DSpace 3.4, DSpace 4.3 or DSpace 5.1 to ensure your site is secure. Several of these security vulnerabilities also affect sites which are running DSpace 1.x.x releases. Per our DSpace Software Support Policy, all DSpace 1.x.x versions are now End-Of-Life.

If you are considering an upgrade from DSpace 1.x.x, note that, as of DSpace 5, your existing data (i.e. database contents, search/browse indexes) will now be automatically upgraded from ANY prior version of DSpace. Therefore, you may wish to consider upgrading directly to DSpace 5.1, as the 5.x upgrade process is simplified.

Summary

DSpace 3.4 is a security fix release to resolve several issues located in DSpace 3.3 or below. As it only provides security-fixes, DSpace 3.4 should constitute an easy upgrade from DSpace 3.x for most users. No database changes or additional configuration changes should be necessary when upgrading from DSpace 3.x to 3.4.

This release addresses the following security issues discovered in DSpace 3.x and below:

- XMLUI Security Fixes
    - *[HIGH SEVERITY] XMLUI Directory Traversal Vulnerabilities* (DS-2445 - requires a JIRA account to access for two weeks, and then will be public): These vulnerabilities allow someone to potentially access *any file* on your local filesystem which is readable to the Tomcat user account. This includes files which are unrelated to DSpace or Tomcat, but are readable to all users on the filesystem (e.g. /etc/passwd, /etc/hosts, etc.). This also includes Tomcat configuration files (which may or may not contain passwords). These vulnerabilities have existed since DSpace 1.5.2.
        - Discovered by: Khalil Shreateh, with additional (related) vulnerabilities discovered by the DSpace Committer Team
    - In some configurations of Tomcat, simply removing any "allowLinking=true" settings from your Tomcat's <Context> configuration will limit the directory traversal vulnerability's severity to only allow access to files within the XMLUI web application directory. In addition, the Tomcat documentation details "allowLinking=true" as a possible security concern. However, you still must upgrade or patch your DSpace in order to completely resolve this vulnerability.
- JSPUI Security Fixes
    - *[MEDIUM SEVERITY] JSPUI Directory Traversal Vulnerability* (DS-2448 - requires a JIRA account to access for two weeks, and then will be public): This vulnerability allows someone to potentially access any file within the JSPUI web application directory (e.g. WEB-INF/web.xml). This vulnerability is believed to have existed in all prior versions of DSpace.
        - Discovered by Khalil Shreateh
    - *[LOW SEVERITY] Cross-site scripting (XSS injection) is possible in JSPUI Recent Submissions listings* (DS-1702 - requires a JIRA account to access for two weeks, and then will be public): This vulnerability could allow a depositor/submitter to embed dangerous Javascript code into the metadata of a new submission, thus causing that code to be run across other user accounts. However, this

vulnerability is only possible by someone with privileges to add content to your DSpace site. This vulnerability has existed since DSpace 1.5.x.
    - Discovered by: Jean-Paul Zhao of University of Toronto
- *[LOW SEVERITY] Cross-site scripting (XSS injection) is possible in JSPUI Discovery search form* (DS-2044 - requires a JIRA account to access for two weeks, and then will be public): This vulnerability could allow someone to embed dangerous Javascript code into links to search results. If a user was emailed such a link and clicked it, the javascript would be run in their local browser. This vulnerability has existed since DSpace 3.x
    - 4.x / 5.x vulnerability discovered by Gabriela Mircea of McMaster University and Khalil Shreateh
    - 3.x vulnerability discovered by Iyas Orak of Biznet Bilisim A.S.

Upgrade Instructions

- For upgrade instructions for 3.x to 3.4 please see Upgrading From 3.0 to 3.x.
- If you are upgrading from 1.8.x to 3.4, please see Upgrading From 1.8.x to 3.x
- For general upgrade instructions, please see Upgrading a DSpace Installation

No new features in DSpace 3.4

3.4 is a bug-fix / security-fix release. This means it includes **no new features** and only includes the above listed security fixes

For a list of all new 3.x Features, please visit the DSpace Release 3.0 Notes.

Changes

The following security fixes were released in 3.4. All of these tickets require a valid JIRA account to view the details:

- DS-1702 - Cross-site scripting (XSS injection) is possible in JSPUI Recent Submissions listings
- DS-2044 - Cross-site scripting (XSS injection) is possible in JSPUI Discovery search form
- DS-2445 - XMLUI Directory Traversal Vulnerabilities
    - Also resolves related, minor theme access issues DS-1896 and DS-2130.
- DS-2448 - JSPUI Directory Traversal Vulnerability

Organizational Details

Release Coordination

- Release Coordinator: Committers Team (shared coordination) led by Tim Donohue

Timeline and Proceeding

Release Timeline:

- Release Date: February 24, 2015