

DSpace Release 5.1 Status

Version 5.1

Support for DSpace 5 ended on January 1, 2023. See [Support for DSpace 5 and 6 is ending in 2023](#)

DSpace 5.1 was officially released to the public on February 25, 2015.

 DSpace 5.1 can be downloaded immediately from:

- <https://github.com/DSpace/DSpace/releases/tag/dspace-5.1>

More information on the 5.1 release (and the 5.x platform in general) can be found in the [5.x Release Notes](#).

We highly recommend any users of DSpace 5.x upgrade to 5.1

 DSpace 5.1 contains security fixes for both the XMLUI and JSPUI. To ensure your 5.x site is secure, **we highly recommend all DSpace 5.x users upgrade to DSpace 5.1**.

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.

- 1 [Summary](#)
 - 1.1 [Upgrade Instructions](#)
- 2 [No new features in DSpace 5.1](#)
- 3 [Changes](#)
- 4 [Organizational Details](#)
 - 4.1 [Release Coordination](#)
 - 4.2 [Timeline and Proceeding](#)

Summary

DSpace 5.1 is a security and bug fix release to resolve several issues located in DSpace 5.0. As it only provides only bug fixes, DSpace 5.1 should constitute an easy upgrade from DSpace 5.0 for most users. No database changes or additional configuration changes should be necessary when upgrading from DSpace 5.0 to 5.1.

This release addresses the following security issues discovered in DSpace 5.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.](#)

In addition, this release fixes a variety of minor bugs in the 5.0 release. For more information, see the [Changes section](#) below.

Upgrade Instructions

- For upgrade instructions from ANY PRIOR VERSION to 5.1, please see [Upgrading DSpace](#)

No new features in DSpace 5.1

5.1 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 5.x Features, please visit the [5.x Release Notes](#).

Changes

The following security fixes were released in 5.1. 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

The following bug fixes were released in 5.1.

key	summary	type	created	updated	due	assignee	reporter	priority	status	resolution
Unable to locate Jira server for this macro. It may be due to Application Link configuration.										

key	summary	type	created	updated	due	assignee	reporter	priority	status	resolution
Unable to locate Jira server for this macro. It may be due to Application Link configuration.										

Organizational Details

Release Coordination

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

Timeline and Proceeding

Release Timeline:

- Release Date: February 25, 2015