

# DSpace 6.4 Release Status

**Support for DSpace 6 will be ending on July 1, 2023.** See [Support for DSpace 5 and 6 is ending in 2023](#)  
DSpace 6.4 was officially released to the public on July 28, 2022



DSpace 6.4 can be downloaded immediately from:

- <https://github.com/DSpace/DSpace/releases/tag/dspace-6.4>

More information on the 6.3 release (and the 6.x platform in general) can be found in the [6.x Release Notes](#).

Upgrade instructions can be found at [Upgrading DSpace](#)

We highly recommend ALL users of DSpace 6.x upgrade to 6.4



DSpace 6.4 contains security fixes for both the JSPUI and XMLUI. To ensure your 6.x site is secure, **we highly recommend ALL DSpace 6.x users upgrade to DSpace 6.4!**

DSpace 6.4 upgrade instructions are available at: [Upgrading DSpace](#)

## Security fixes include:

- [HIGH] [CVE-2022-31195](#) (impacts XMLUI and JSPUI): *Path traversal vulnerability in Simple Archive Format package import (ItemImportService API). This means a malicious SAF (simple archive format) package could cause a file/directory to be created anywhere the Tomcat/DSpace user can write to on the server. This path traversal is only possible by a user with special privileges (Administrators or someone with command-line access to the server).*
  - Reported by Johannes Moritz of Ripstech
- [HIGH] [CVE-2022-31194](#) (impacts JSPUI only) : *The JSPUI resumable upload implementations in SubmissionController and FileUploadRequest are vulnerable to multiple path traversal attacks, allowing an attacker to create files/directories anywhere on the server writable by the Tomcat /DSpace user, just by modifying some request parameters during submission. This path traversal can only be executed by a user with submitter rights.*
  - Reported by Johannes Moritz of Ripstech
- [HIGH] [CVE-2022-31193](#) (impacts JSPUI only) : *The JSPUI controlled vocabulary servlet is vulnerable to an open redirect attack, where an attacker can craft a malicious URL that looks like a legitimate DSpace/repository URL. When that URL is clicked by the target, it redirects them to a site of the attacker's choice.*
  - Reported by Johannes Moritz of Ripstech
- [MODERATE] [CVE-2022-31191](#) (impacts JSPUI only) : *The JSPUI spellcheck "Did you mean" HTML escapes the data-spell attribute in the link, but not the actual displayed text. Similarly, the JSPUI autocomplete HTML does not properly escape text passed to it. Both are vulnerable to Cross Site Scripting (XSS).*
  - Reported by Hassan Bhuiyan, Brunel University London
- [MODERATE] [CVE-2022-31192](#) (impacts JSPUI only) : *The JSPUI "Request a Copy" feature is vulnerable to Cross Site Scripting (XSS) attacks.*
  - Reported by Andrea Bollini of 4Science
- [LOW] [CVE-2022-31189](#) (impacts JSPUI only) *When an "Internal System Error" occurs in the JSPUI, then entire exception (including stack trace) is available. Information in this stacktrace may be useful to an attacker in launching a more sophisticated attack.*
  - Reported by Johannes Moritz of Ripstech
- [LOW] [CVE-2022-31190](#) (impacts XMLUI only) *Metadata of withdrawn Items is exposed to anonymous users in XMLUI.*
  - Reported by David Cavrenne of Atmire

## Major bug fixes include:

- Fix Mirage 2 build broken by disappearance of JRuby gems [torquebox.org](#) mirror: [#8292](#)
  - Requires some action on sites with heavily customized JavaScript or stylesheets, see [Mirage 2's readme.md](#)
- Replace log4j with [reload4j](#): [#8144](#)
  - Note: this may impact custom modules pulled into your poms if they pull in log4j v1. We recommend only using reload4j.
- Implement GDPR-compliant statistics anonymization for Solr: [DS-4440 \(#2693\)](#)
- Update Sherpa Romeo integration for API v2: [DS-3940 \(#2739\)](#), [DS-4377 \(#2567\)](#)
- Add utility to [migrate legacy pre-6.x Solr statistics IDs to UUIDs](#): [DS-4075 \(#2260\)](#)
- Various improvements to Docker configuration and deployment: [DS-4356 \(#2542\)](#), [DS-4355 \(#2540\)](#), [DS-4349 \(#2534\)](#), [DS-4346 \(#2523\)](#), [DS-4321 \(#2476\)](#), [DS-4336 \(#2510\)](#), [DS-4126 \(#2307\)](#), [DS-4142 \(#2322\)](#), [DS-4012 \(#2218\)](#)
- Database fixes:
  - Change maxwait default to 10 seconds: [DS-4562 \(#7895\)](#)
  - Upgrade DBCP2 dependencies: [DS-4574 \(#3162\)](#)
  - Fix OAI-PMH identify verb when using Oracle RDBMS: [DS-3453 \(#2112\)](#)
  - Migrate update-sequences.sql script to dspace database command: [DS-4167 \(#2362\)](#)
- XMLUI fixes:
  - Add noindex HTML meta tag to prevent robots from indexing private items: [DS-1980 \(#5346\)](#)
  - Update Mirage2 build to support Node.js 14 LTS: [#8331](#)
  - Update confidence when manually editing authority controlled metadata values: [DS-4580 \(#7913\)](#)
  - Fix breaking of feedback link on sites without a sub-domain: [DS-4362 \(#7701\)](#)
  - Improve performance of item counter (aka "strengths"): [DS-3976 \(#7323\)](#)
  - Fix jumping to a specific year in search results when site is not using the default sort order: [DS-4208 \(#7548\)](#)
  - Fix word-break CSS class: [DS-4190 \(#2374\)](#)
  - Improvements and bug fixes to starts\_with parameter on browse pages: [DS-4201](#), [DS-3945 \(#2113\)](#)
  - Re-enable HTTP Ranges support: [DS-4579 \(#3228\)](#)
  - Fix Known/Supported labels in UploadStep/UploadWithEmbargoStep: [DS-4293 \(#2465\)](#)
  - Fix Discovery label for metadata values under authority control: [DS-2852 \(#1800\)](#)
  - Fix incorrect escaping of citation\_ meta tags: [DS-4135 \(#2317\)](#)
  - Fail gracefully if the Creative Commons API is down: [DS-2569 \(#2977\)](#)
  - Respect primary bitstreams with text/html mime types in Mirage2 item view: [DS-3888 \(#2021\)](#)

- Use null for empty language when editing item metadata: [DS-4169 \(#2350\)](#)
- Properly show results for 0-9 link in Browse: [DS-4291 \(#2463\)](#)
- Fix missing date values while faceting: [DS-3791 \(#1901\)](#)
- Fix support for custom `sitemap.xml` in Mirage 2: [DS-3545 \(#1690\)](#)
- Fix broken "reset" button in Discovery advanced search filters: [#8330](#)
- Fix incorrect totals on Discovery "view more" page: [DS-3881 \(#2371\)](#)
- JSPUI fixes:
  - Improve results in item mapper: [#2649](#)
  - Make sure that transactions are committed in curation tasks: [DS-4564 \(#3087\)](#)
  - Performance enhancement for large uploads: [DS-4551 \(#2964\)](#)
  - Port ORCID author lookup integration to JSPUI: [DS-2715](#), [DS-4439 \(#2710\)](#)
  - Fix bug in JSPUI Shibboleth session renewal: [DS-3444 \(#2358\)](#)
  - Add missing keys for search filters in `Messages.properties`: [DS-4029 \(#2556\)](#)
  - Fix issue with duplicate headers when bitstream title has a comma: [DS-4340 \(#2513\)](#)
- Other API-level fixes (affecting all UIs):
  - Improve Solr search results for Discovery *contains* queries by using double quotes instead of brackets: [DS-4271 \(#7611\)](#)
  - Add a check to make sure the source and target collections are not the same when moving an item: [#8055](#)
  - Avoid exporting metadata of mapped Item more than once: [#7988](#)
  - Make sure "Save and Exit" in workflow actually saves changes to the database: [DS-4157 \(#7499\)](#)
  - Fix `NullPointerException` in ORCIDv2 API responses with missing data: [DS-3998 \(#7345\)](#)
  - Fix `NullPointerException` when selecting items published today in initial questions step: [DS-4238 \(#7668\)](#)
  - Fix `NullPointerException` on empty sub-communities in *metadata-export*: [DS-4211 \(#2396\)](#)
  - Fix "homepage" Discovery configuration not being used due to missing IDs: [DS-3725 \(#7072\)](#)
  - Fix ingesting items without a license not using the default license: [DS-3643 \(#6992\)](#)
  - Prevent empty string assignment for language when importing a SAF bundle: [DS-4493 \(#2753\)](#)
  - Fix searching for text values containing diacritics: [DS-4034 \(#2276\)](#)
  - Fix for view permissions when Anonymous is a sub-group: [DS-4534 \(#2832\)](#)
  - `FindByValue` should pass in value, not qualifier: [DS-4073 \(#2699\)](#)
  - Fix exception when harvesting by UUID: [DS-4353 \(#2537\)](#)
  - Fix `NullPointerException` in "request a copy" function: [DS-4032 \(#2452\)](#)
- REST API fixes:
  - Fix Maven build issue due to blocking of plaintext HTTP repositories: [#3247](#)
  - Return items in deterministic order: [DS-3849 \(#2501\)](#)
  - Improve performance of collections endpoints: [DS-4342 \(#2516\)](#)
  - Fix schema registry lookup with null qualifier: [#7993](#)

#### Minor improvements include:

- Limit the usage of `PDFBoxThumbnail` media filter to PDFs: [DS-3873](#)
- Update PDFBox version: [#2742](#)
- Update spider user agent file for more accurate Solr usage statistics: [DS-4587 \(#3333\)](#)
- Update JavaScript dependencies: [DS-4508 \(#2918\)](#)
- Remove non-existent command from OAI's CLI help: [DS-4260 \(#2439\)](#)
- Fix Discovery index command when using the "-c" (clean) option: [DS-4393 \(#2606\)](#)
- Fix issue with `bulkedit.ignore-on-export` parameter on `DSpaceCSV`: [#2661](#)
- Improve `dspace structure-builder` error messages: [DS-4087 \(#2681\)](#)
- Remove GeolP download Ant target, reconfigure for external provision: [DS-4409 \(#2652\)](#)
- Restores `getSize()` in Bitstream for replication task suite: [DS-3895 \(#2683\)](#)
- Remove unnecessary second Context in `RDFConsumer`: [#8152](#)
- Fix minor security issue with HTML links using `target="_blank"`: [DS-3891 \(#7238\)](#)
- Correctly remove Handle server lock file: [DS-3946 \(#2114\)](#)
- Make automatic Discovery re-indexing configurable: [DS-3658 \(#2184\)](#)
- Allow configuring max results per page in search: [DS-4120 \(#2306\)](#)
- Improve OAI performance for large installs: [DS-4136 \(#2320\)](#)
- Avoid crosswalking invalid publish dates for Google Scholar: [DS-4104 \(#2294\)](#)
- Bitstreams should keep their formats when being versioned: [DS-4078 \(#2261\)](#)
- Only execute ImageMagick `identify` on the first page of PDF: [DS-3664 \(#2201\)](#)
- Allow OAI Harvester to continue if it encounters an Item missing a handle: [DS-3939 \(#2106\)](#)
  - Note: the OAI Harvester Consumer has been completely removed from the DSpace codebase and should be removed from any configuration files referencing it: [DS-4129 \(#2314\)](#).

View the [full list of changes for DSpace 6.4 on GitHub](#).

## 6.4 Acknowledgments

The 6.4 release was led by [Alan Orth](#), [Kim Shepherd](#), [Nicholas Woodward](#) and [Hrafn Malmquist](#) (of Cottage Labs).

The following individuals provided tests, code, bug fixes, or review to the 6.4 release (in alphabetical order by given name): Alan Orth, Alexander Sulfrian, Andrea Bollini, Andrea Jenis Saroni, Andrew Wood, Anis, Bram Luyten, Chris Herron, Chris Wilper, Cornelius Matjka, Francesco Pio Scognamiglio, Giuseppe Digilio, Hrafn Malmquist, Huma Zafar, Iordanis Kostelidis, Istvan Vig, Jonas Van Goolen, Kim Shepherd, Kristof De Langhe, Leonardo Guerrero, Lotte Hofstede, Luigi Andrea Pascarelli, Mark H. Wood, Martin Walk, Nicholas Woodward, Pascal-Nicolas Becker, Paulo Graça, Philip Vissenaekens, PTrottier, Saiful Amin, Samuel, santit96, ssolim, Terry Brady, Tim Donohue, Toni Prieto.

