DRUPAL
DEVELOPER DAYS
Burgas, Bulgaria - 2024

D7Security

Drupal 7 long term support
Klaus Purer

About me

Klaus Purer ("klausi")

Principal Engineer at Jobiqo

Doing Drupal for 16 years

Interests: Information Security, Programming Languages, Devops, Performance, GraphQL, REST, Coder

https://klau.si

https://mastodon.social/@klausi

Outline

Status Drupal 7

Options for Drupal 7 site owners

D7Security project

Discussion

Drupal usage

Weekly project usage
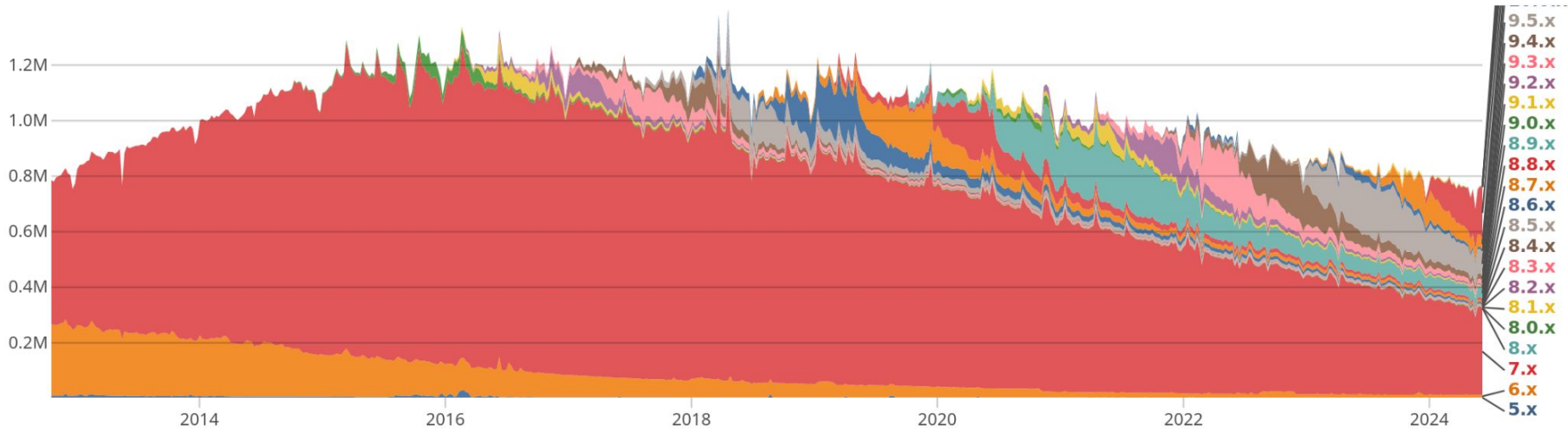
Drupal Usage 2024

Data from 2024-06-17

Drupal 5	171	0%
Drupal 6	8,550	1%
Drupal 7	313,698	41%
Drupal 8	71,324	9%
Drupal 9	130,434	17%
Drupal 10	234,170	31%
Drupal 11	1,682	0%
Drupal 8..11	437,610	58%
Total	760,060	100%

Drupal 7 status on drupal.org PSA-2023-06-07

- Official end-of-life date is Jan 5th 2025
- Reduced support for moderately critical Drupal 7 security issues
    - Issues will be moved to the public issue queue
- Unsupported Drupal 7 modules and themes cannot be set to supported again
- Security fixes will no longer be provided for Drupal 7 Windows-only issues

Options for Drupal 7 site owners

- Migrate to Drupal 10
- Migrate to Backdrop CMS
- Migrate to another system (Wordpress etc)
- Stay on Drupal 7 and buy LTS contract
- Stay on Drupal 7, patch security problems yourself (and share fixes with D7Security)

The **Drupal 7 Soft Landing Initiative** provides good guidance on this!

https://www.drupal.org/community-initiatives/drupal-7-soft-landing-initiative
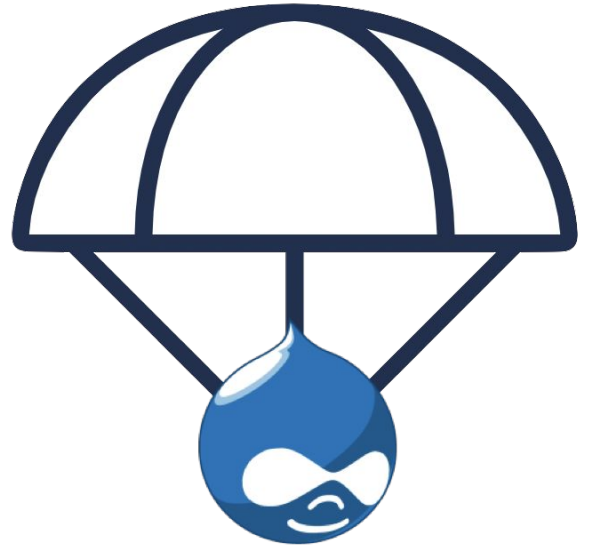
Migrate to Drupal 10

Pros:

- Actively supported system
- Benefit from all the improvements

Cons:

- High effort, requires rewrite of custom code and migration strategy

Drupal Module Upgrader for automated conversions

https://www.drupal.org/project/drupalmoduleupgrader

Retrofit: Run Drupal 7 code in Drupal 10

https://retrofit-drupal.com/

Migrate to Backdrop CMS

Pros:

- Actively supported system
- Less effort than migrating to Drupal 10

Cons:

- Small open source project not widely known
- Some migration effort (no drop-in replacement for Drupal 7)

Migrate to another system

Pros:

- Freedom to pick the best tool for the job
- Good match when changing the project anyway

Cons:

- High effort
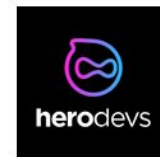- Other tools are not as powerful out of the box as Drupal

Drupal 7 commercial LTS support

Currently 3 officially endorsed providers listed on drupal.org, but their offering is intransparent

Pros:

- No migration, no rewrite
- Fulfills security compliance requirements

Cons:

- Unclear how the providers will work
- Cost?
- Can only postpone modernization efforts

Drupal 7 self support

Pros:

- You are a core and security maintainer now
- Low initial effort, no migration

Cons:

- You are a core and security maintainer now
- Risky, how do you mitigate security vulnerabilities?
- Maintenance cost
- Compliance problems
- Can only postpone modernization efforts

D7Security: History and Background

"Drupal 7 branches of unsupported modules and themes are no longer eligible for new maintainership"

– Drupal Security Team in Drupal 7 end of life announcement PSA-2023-06-07

- No shared space to publish Drupal 7 contrib releases, forbidden by policy on drupal.org
- No mechanism to inform Drupal 7 site owners when an unsupported project would have a new release with a security fix
- No clear Drupal 7 extended support plan or vendors on drupal.org

What is the D7Security project?

- Mission: Provide unofficial support for Drupal 7

- Open Source Project on Gitlab.com

- Unofficial and independent from drupal.org, the Drupal Association and the Drupal Security Team

- Contributors from multiple companies publish Drupal 7 contrib projects we use and care about

- Provides an update status server to notify you of security updates

- Not Backdrop CMS

How does D7Security work?

- Site owners need to install a client module

- Serverless; Static update XML files

- Gitlab CI runner scripts that package projects (info file timestamps and versions)
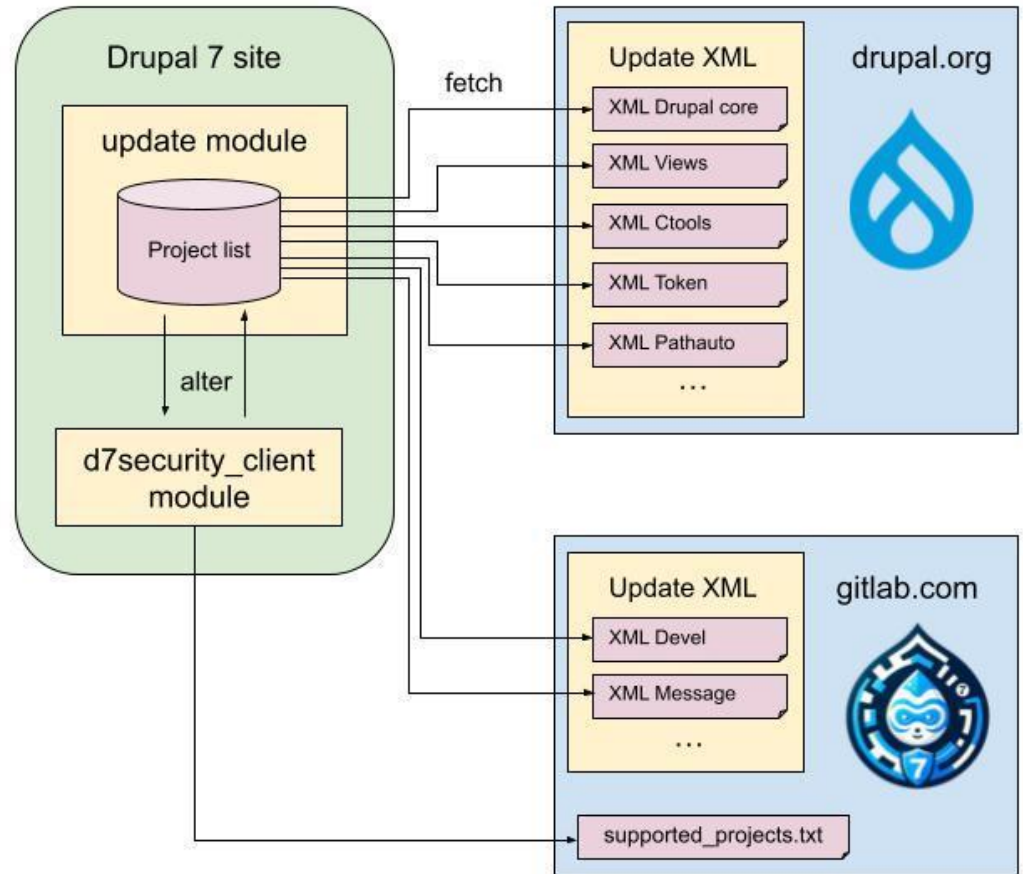
d7security_client

```php
/**
 * Implements hook_system_info_alter().
 */
function d7security_client_system_info_alter(array &$info, \stdClass $file, string $type) {
  …
  if (!empty($info['project']) && in_array($info['project'], $supported_projects)) {
    $info['project status url'] = variable_get('d7security_client_project_status_base_url',
      'https://gitlab.com/d7security/d7security/-/raw/main'
    );
  }
  …
}
```

Drush support

You need to enable the d7security_client module first.

- drush pm-updatestatus (drush ups) ✅
- drush pm-update (drush up) ✅
- drush pm-download (drush dl)
  - drush dl coffee ❌
  - drush dl coffee --source=https://gitlab.com/d7security/d7security/-/raw/main ✅

Drush make support

```
; D7Security project hosted at https://gitlab.com/d7security/coffee

projects[coffee][version] = 2.4

projects[coffee][type] = module

projects[coffee][download][type] = file

projects[coffee][download][url] =
https://gitlab.com/api/v4/projects/55398429/packages/generic/coffee/7.x-2.4/coffee-7.x-2.4.tar.gz
```

User Guide

Dashboard | Content | Structure | Appearance | People | Modules | Configuration | Reports | Help   Hello **admin**   Log out

Add content   Find content   Edit shortcuts

Home » Administration » Reports

Available updates ✿

LIST | UPDATE | SETTINGS

Here you can find information about available updates for your installed modules and themes. Note that each module or theme is part of a "project", which may or may not have the same name, and might include multiple modules or themes within it.

➕ Install new module or theme

Last checked: 10 hours 9 min ago (Check manually)

Drupal core

Drupal core 7.99   Up to date ✓

Includes: Bartik, Block, Color, Comment, Contextual links, Dashboard, Database logging, Field, Field SQL storage, Field UI, File, Filter, Help, Image, List, Menu, Node, Number, Options, Overlay, Path, RDF, Search, Seven, Shortcut, System, Taxonomy, Text, Toolbar, Update manager, User

Modules

d7security_client 7.x-1.0   Up to date ✓

Includes: D7Security client

Devel 7.x-1.8   Up to date ✓

Includes: Devel

⬢ D7Security / devel / **Releases**

Released date ⌄ | ⬇   **New release**

devel 7.x-1.8   ✎

⌄ Assets 6
  📄 Source code (zip) ⬇
  📄 Source code (tar.gz) ⬇   **Unpacked source code files, do not use!**
  📄 Source code (tar.bz2) ⬇
  📄 Source code (tar) ⬇

Other
  🔗 devel-7.x-1.8.zip ⬀   **Properly packaged release, use them!**
  🔗 devel-7.x-1.8.tar.gz ⬀

Evidence collection

📋 7.x-1.8-evidences-7330845.json ⬀ ••• cad630c8 📋

🕐 Collected 6 days ago

Regular bugfix release of Devel for Drupal 7. List of changes: 7.x-1.7...7.x-1.8

Warning: Do not use the default source code assets as they don't contain info file timestamps. Use the properly packaged devel-7.x-1.8.tar.gz or devel-7.x-1.8.zip.

⊶ 449104b5   ⬒ 7.x-1.8   Released 6 days ago by 👤

Currently supported projects

Preconditions:

- The Drupal 7 project is unsupported on drupal.org

- A member of D7Security wants to support it

Current list from machine-readable supported_projects.txt:

```
coffee  d7security_client  devel

ldap  message  simple_gmap
```

Values and Philosophy

- No branding of D7Security as a Drupal Classic fork

- We accept that Drupal 7 is legacy software

- Ensuring stability, security and PHP compatibility: no new features or refactoring

- Respect and best intentions towards Drupal Security Team, Drupal Association, Drupal 10 maintainers, Backdrop CMS - they are our partners

- We accept that security fixes will be released for Drupal 10 modules first

- Drupal Code of Conduct

Reporting Drupal 7 Security vulnerabilities

🚨 All security reports against Drupal 7 core and contrib projects must still be reported via security.drupal.org first! 🚨

Security Advisories

- Similar to drupal.org
- Summarize vulnerability, risk, impact, mitigation
- Published at d7security.org/security-advisories
- Code names, for example
  D7SECURITY-SA-CONTRIB-2024-001

Coffee - Moderately critical - Cross Site Scripting - D7SECURITY-SA-CONTRIB-2024-001

2024/02/28

Project: Coffee

Security risk: Moderately critical 13⁄25 AC:Basic/A:Admin/CI:Some/II:Some/E:Theoretical/TD:All

Vulnerability: Cross Site Scripting

Affected versions: <7.x-2.4

Description:

The Coffee module helps you to navigate through the Drupal admin menus faster with a shortcut popup.

The module doesn't sufficiently escape menu names when displaying them in the popup, thereby exposing a XSS vulnerability.

This vulnerability is mitigated by the fact that an attacker must have a role with the permission "Administer menus and menu links".

See also Coffee - Moderately critical - Cross Site Scripting - SA-CONTRIB-2024-011.

Communication Channels

There is a #d7security channel in Drupal Slack.

The main communication channel for coordination are Gitlab issues in the D7Security project

Subscribe to notifications on the project announcement Gitlab issue, which serves as a newsletter.

D7Security members and joining

Klaus Purer ([klausi on drupal.org](), [klausi1 on gitlab.com]())

Ivan Tibezh ([tibezh on drupal.org](), [tibezh on gitlab.com]())

Juraj Falat ([durifal on drupal.org](), [durifal on gitlab.com]())

Andrii Cheredn ([andriic on drupal.org](), [onesixromcom on gitlab.com]())

John Locke ([freelock on drupal.org](), [freelock_john on gitlab.com]())

Jen Lampton ([jenlampton on drupal.org](), [jenlampton on gitlab.com]())

Gregor Sýkora ([gresko8 on drupal.org](), [gresko2 on gitlab.com]())

Greg Knaddison ([greggles on drupal.org](), [gknaddison on gitlab.com]())

Allison Vorthmann ([allisonherodevs on drupal.org](), [aavorthmann on gitlab.com]())

Caroline Boyden ([cboyden on drupal.org](), [cboyden on gitlab.com]())

Feel free to reach out to me if you are interested!

D7Security after January 2025

- Fork Drupal 7 core and projects to Gitlab.com (once unsupported on drupal.org)
- Establish private Gitlab security issue process
- Collaborate with commercial providers and developers to release security fixes

Risks of running Drupal 7 beyond 2025

- Drupalgeddon-like vulnerabilities (remote code execution)
- Commercial vendors don't collaborate and release different Drupal 7 fixes
- Delays in porting Drupal 10 security fixes to Drupal 7

Where we need help

- Implement the design for the website
- Marketing: blog posts how you work with D7Security
- Core (and contrib) maintainers after Jan 2025, none of the current core maintainers are interested so far
- Commitment from the commercial vendors how they will collaborate with D7Security (or not)

Resources and Links

- Website www.d7security.org (work in progress)
- Wiki https://gitlab.com/d7security/d7security/-/wikis/home
- Newsletter https://gitlab.com/d7security/d7security/-/issues/2
- Discussion https://gitlab.com/d7security/d7security/-/issues/1
- Slack #d7security https://app.slack.com/client/T06GX3JTS/C06AP6GE05P
- Start of the discussion on drupal.org https://www.drupal.org/project/ideas/issues/3408125
- D7EOL Podcast episode https://www.youtube.com/watch?v=hNI73M0ftOM

Any questions?

- What do Drupal 7 users and developers need in addition to D7Security?
- What is the best way to proceed after January 2025 when D7Security will fully take over from drupal.org?
- How can we reach interested Drupal 7 community members?

Thank you for joining us!

Stay connected with **Drupal Bulgaria Association** for more exciting events, news, and updates!

Also visit our website: **https://ddd24.drupalcamp.bg**

And don't forget to visit our **sponsors' stands**.

Their support helps make events like this possible!