



Dasharo User Group #11 🎉 and Developers vPub 0x10 🍺



Dasharo User Group #11

Dasharo Community Status



Agenda

- Dasharo Team Events Roadmap
- Dasharo Issues repo stats
- Dasharo coreboot and edk2 repos stats
- Dasharo coreboot upstreaming
- Dasharo Matrix stats
- Dasharo Infrastructure changes

Dasharo Team Events Roadmap Q3'25

subject to change



Year 2025

Jul

Aug

Sep

Oct

Nov

Dec

Dasharo

DUG#11 &
vPub 0x10

Qubes OS
Summit 2025

DUG#12 &
vPub 0x11

Linux Plumbers
Conference

Zarhus Dev
Meetup #2

Zarhus

Zarhus Dev
Meetup #3

Pace Enterprise
Training

HWIO NL

Mastering
UEFI Secure Boot
and Intel Root of
Trust Technologies

Dasharo Team Events Roadmap | September 2025 | CC-BY-SA-4.0

Upcoming 2025

- [2025-09-18 Dasharo User Group 11 & Developers vPub 0x10](#)
- [2025-09-26-28 Qubes OS Summit 2025](#)
- [2025-11-04 Zarhus Developers Meetup 3](#)
- [2025-12-11 Dasharo User Group 12 & Developers vPub 0x11](#)

2025

- [Bug Bounty Program Live Demo](#)
- [Zarhus Developers Meetup 2](#)
- [Dasharo User Group 10 & Developers vPub 0xF](#)
- [Zarhus Developers Meetup 1](#)
- [Dasharo User Group 9 & Developers vPub 0xE](#)
- [FOSDEM 2025](#)
- [Xen Project Winter Meetup](#)

2021

- [Yocto Project Virtual Summit](#)
- [Dasharo OSF vPub Fall 2021 \(aka 3mdeb vPub vol. 3\)](#)
- [Linux Secure Launch - TrenchBoot Summit](#)
- [OpenPOWER Summit](#)
- [TPM.dev 2021 MiniConf](#)
- [Linux Plumbers Conference](#)
- [EuroBSDCon](#)
- [Qubes OS Minisummit](#)
- [OpenPOWER Community Call](#)
- [Zephyr Developer Summit](#)
- [Xen Developer & Design Summit](#)
- [Yocto Project Summit 2021](#)
- [NGI Forum 2021](#)
- [vPub 0x2](#)
- [TrenchBoot Developers Forum 2021](#)
- [vBeer 0x1](#)
- [FOSDEM 2021](#)

<https://events.3mdeb.com>

DASHARO USER GROUP 10

Dasharo User Group (DUG) #10 & Dasharo ...

by 3mdeb

Playlist • 10 videos • 2 views

The Dasharo User Group (DUG) is an important forum for users of Dasharo to come together, share their kno ...[more](#)

[▶ Play all](#)

ZARHUS DEVELOPERS MEETUP #2

Zarhus Developers Meetup #2

by 3mdeb

Playlist • 6 videos • 24 views

The Zarhus Developers Meetup is an event organized by 3mdeb that brings together users and developers ...[more](#)

[▶ Play all](#)

Link to DUG#10 and vPub 0xF [YouTube playlist](#) and [slides](#).

Link to ZDM#2 [YouTube playlist](#) and [slides](#).

Qubes OS Summit '25

September 26-28

The Social Hub
Berlin, Germany

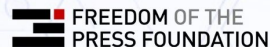
Learn more at:

events.dasharo.com/event/2/qubes-os-summit-2025

Conference organizers



Platinum Partners



Gold Partners



Silver Partners



Friday 26. September

10:00 AM

10:00 Welcome to Qubes OS Summit 2025 Day 1

AM  Piotr Król, Marek Marczykowski-Górecki

25min

We're excited to open this year's summit with a warm welcome, bringing together the community to reconnect, collaborate, and exchange ideas in the spirit of trust and transparency.

...

Social Hub Main Room

10:30 AM

10:30 Qubes OS 4.3 development update

AM Marek Marczykowski-Górecki

30min

This presentation will review what is coming in Qubes OS 4.3. Many of the mentioned features will get separate dedicated presentation.

Social Hub Main Room

11:55 AM

11:55 Have your Qubes and keep it?

AM Matthias Ferdinand

30min

Using Qubes OS as admin workstations in our corporate IT environment requires some changes on both sides, and we try to not to ruin security on either side. Surely there is room for improvement.

Social Hub Main Room

12:30 PM

12:30 Qubes Air: Hardware, Firmware, and Architectural Foundations

PM  Michał Żygowski

30min

Qubes OS has traditionally been recognized for its excellence on personal laptops and desktops, securely compartmentalizing computing tasks. Extending Qubes OS to modern AMD server platforms introduces exciting opportunities but also unique security considerations. This foundational talk explores selected...

Social Hub Main Room

<https://events.dasharo.com/event/2/qubes-os-summit-2025>

2:30 PM

2:30
PM

Rethinking the compartmentalization experience

 Alyssa Ross

30min

I'm the founder and project lead of [Spectrum](#), an in-development compartmentalized operating system. It's heavily inspired by Qubes OS, but also does a lot of things differently. This talk will highlight differences between Spectrum and Qubes OS, with a particular focus on user and developer experience, explain the reasoning behind those differences, and highlight what Qubes OS might be able to take from Spectrum's experience doing...

Social Hub Main Room

3:05 PM

3:05
PM

Qubes Air: Opinionated Value Proposition for Security-Conscious Technical Professionals

 Piotr Król

30min

Building on "Qubes Air: Hardware, Firmware, and Architectural Foundations" talk, this session outlines an opinionated vision of Qubes Air vertical integration, explicitly addressing the needs of security-conscious technical professionals like security researchers, developers, privacy advocates, and SMEs operating in the surrounding ecosystem. Grounded in Kicksecure/Whonix [persona](#) and [threat model](#), it emphasizes potential vertical integrati...

Social Hub Main Room

3:45 PM

3:45
PM

Alternative options to signify qube ownership of windows/widgets/... (including more colors)

 Ali Mirjamali

30min

My personal quest of implementing alternative approaches to the default 8 labels (colors):

- Tools to create/manage additional label colors (and why it matters)...

Social Hub Main Room

4:20 PM

4:20
PM

Qubes OS: Design for Hackers and How To Contribute to GUI Tools

Marta "marmarta" Marczykowska-Górecka

60min

Contributing to GUI tools can be a daunting process: it's not very easy to test things on Qubes OS, the whole OS stack is enormous, and the very idea of designing an interface is quite scary to many developers. It does not have to be that bad, though! In this talk, I will briefly introduce the testing tools Qubes OS has that can be useful for GUI development, explain how to find our design patterns for more consistent GUI applications, and give ...

Social Hub Main Room

<https://events.dasharo.com/event/2/qubes-os-summit-2025>

4:20 PM

4:20 PM Qubes OS: Design for Hackers and How To Contribute to GUI Tools

Marta "marmarta" Marczykowska-Górecka

60min

Contributing to GUI tools can be a daunting process: it's not very easy to test things on Qubes OS, the whole OS stack is enormous, and the very idea of designing an interface is quite scary to many developers. It does not have to be that bad, though! In this talk, I will briefly introduce the testing tools Qubes OS has that can be useful for GUI development, explain how to find our design patterns for more consistent GUI applications, and give ...

Social Hub Main Room

5:25 PM

5:25 PM Using segregation to hyper secure your development environment.

 Rene Malmgren

30min

In the age of an ever increasing threat level, from more and more capable actors, a new set of understanding is needed for industry to secure there critical information, like the development of software, cryptographic money and cryptographic keys that access systems.

Social Hub Main Room

5:55 PM

5:55 PM Qubes OS Summit 2025 - Day 1 closing notes

 Piotr Król

5min

Closing notes

Social Hub Main Room

7:30 PM

7:30 PM Afterparty: TBD

TBD

4h

[Break](#)

Social Hub Main Room

Saturday 27. September

10:00 AM

10:00 AM Welcome to Qubes OS Summit 2025 Day 2

 Piotr Król

10min

- * Day 2 event schedule and organization announcements
- * Shout out to the sponsors

Social Hub Main Room

<https://events.dasharo.com/event/2/qubes-os-summit-2025>

Saturday 27. September

10:00 AM

10:00

AM

10min

Welcome to Qubes OS Summit 2025 Day 2



Piotr Król

- * Day 2 event schedule and organization announcements
- * Shout out to the sponsors

Social Hub Main Room

10:15 AM

10:15

AM

30min

NovaCustom: Intel Boot Guard e-fusing, HSI levels, Capsule Updates and new products



Wessel klein Snakenborg

During this talk, we will highlight our big firmware updates of Q2/Q3-2025. These updates for both current device models as well as older models include support for Intel Boot Guard, improved HSI level achievements and Capsule Updates with support for fwupd/LVFS. On top of that, we will introduce new firmware features, such as the Dasharo ACPI driver and sleep-and-charge ports....

Social Hub Main Room

10:50 AM

10:50

AM

30min

Update on UEFI Secure Boot in Qubes OS

Kamil Aronowski

A review of the progress towards implementing UEFI Secure Boot support in Qubes OS. What we've managed to accomplish since [last year's talk](#). What both technical and non-technical challenges are still out there to be solved.

Social Hub Main Room

11:25 AM

11:25

AM

30min

Can It Run TrenchBoot?



Maciej Pijanowski

TrenchBoot leverages Intel TXT and AMD Secure Startup to provide Dynamic Root of Trust for Measurement (DRTM), enhancing boot security beyond traditional approaches. This talk presents current state of the project and findings from extensive hardware testing.

...

Social Hub Main Room

<https://events.dasharo.com/event/2/qubes-os-summit-2025>

11:25 AM

11:25
AM

Can It Run TrenchBoot?

 Maciej Pijanowski

30min

TrenchBoot leverages Intel TXT and AMD Secure Startup to provide Dynamic Root of Trust for Measurement (DRTM), enhancing boot security beyond traditional approaches. This talk presents current state of the project and findings from extensive hardware testing.

...

Social Hub Main Room

12:00 PM

12:00
PM

Qubes Windows Tools: the present and the future

Rafał Wojdyła

30min

This talk will cover the current state of Qubes Windows integration as well as future plans. Some key points include:

- Development setup: how to develop, debug and contribute to QWT...

Social Hub Main Room

12:35 PM

12:35
PM

Recent Advances in Device Management in Qubes OS

Piotr Bartman-Szwarc

20min

In this talk, I will present the latest improvements in peripheral device handling in Qubes OS, focusing on USB, block devices, and PCI. We'll explore the architectural changes, security implications, and user experience enhancements introduced in recent updates.

Social Hub Main Room

1:00 PM

1:00
PM

Lunch break

Lunch break

1h30min

Break

Social Hub Main Room

2:30 PM

2:30
PM

Qubes OS CI review

Marek Marczykowski-Górecki

30min

Review of how Qubes OS CI evolved over last couple of years. The presentation will include, among other things:

- improvements to openQA setup
- running tests with 4K resolution...

Social Hub Main Room

<https://events.dasharo.com/event/2/qubes-os-summit-2025>

3:05 PM	
3:05 PM 30min	RST Documentation and Localization in Qubes OS m, Tobias Killer From Community Collaboration to Automated Localization: Building a Sustainable Documentation Ecosystem for Qubes OS, what is ahead? Social Hub Main Room
3:40 PM	
3:40 PM 30min	Ansible in Qubes OS Frédéric Pierret In this talk, we will present the integration of Ansible into Qubes OS. Built on the original work by @kushaldas, we extended the implementation with new features and mechanisms, making Ansible as a viable alternative to SaltStack, which until now has been the sole infrastructure-as-code solution in Qubes OS. Social Hub Main Room
4:15 PM	
4:15 PM 30min	Even More Control: What's New With Qubes GUI Tools Marta "mamarta" Marczykowska-Górecka An overview of the new GUI tools and changes in 4.3 Social Hub Main Room
4:50 PM	
4:50 PM 30min	Fast and fresh disposable qubes Ben Grande Have you ever considered that a dangerous file or workflow should be done on a fresh disposable but you always thought it was slow and not worth it, executing the action on the same qube? This will change. No more slowness! No lack of isolation! No reuse of named disposables! Preloaded disposables to the rescue... Social Hub Main Room
5:55 PM	
5:55 PM 5min	Qubes OS Summit 2025 - Day 2 closing notes Piotr Król Closing notes Social Hub Main Room

<https://events.dasharo.com/event/2/qubes-os-summit-2025>

Qubes OS Summit 2025: On-site Tickets

6 available ▾

🕒 **Late** - Available from September 1

€200.00

− 0 +

👕 **Official T-Shirts are now on sale!**

Get your Qubes OS Summit 2025 shirt here: <https://shop.3mdeb.com/shop/merchandise/qubes-os-summit-2025-official-t-shirt/>

If you require an invoice, please contact us at events@3mdeb.com.

Cryptocurrency payments are also accepted — feel free to contact us for more information.

Hide

Qubes OS Summit 2025: Virtual Tickets

▾

Free

Sales ended

Note: Certain sessions at the event may be presented under a **no-streaming / no-recording policy**, and will only be accessible to on-site participants.

<https://events.dasharo.com/event/2/qubes-os-summit-2025>

hardwear.io

NETHERLANDS 2025

Training

Mastering UEFI Secure Boot and Intel Root of Trust Technologies

by

Piotr Król



17-19 NOVEMBER | 9 AM - 5 PM CEST

MARRIOTT HOTEL, AMSTERDAM

<https://hardwear.io/netherlands-2025/training/mastering-uefi-secure-boot-and-intel-root-of-trust-technologies.php>

Dasharo Team Events Roadmap Q1'26-Q2'26

subject to change



Year 2026

Jan

Feb

Mar

Apr

May

Jun

Dasharo

FOSDEM 2026

Open-source firmware
devroom

DUG#13 &
vPub 0x12

DUG#14 &
vPub 0x13

Zarhus Dev
Meetup #4

Zarhus Dev
Meetup #5

Zarhus

Dasharo Team Events Roadmap | September 2025 | CC-BY-SA-4.0



Use QR code to get news about upcoming OST2 classes:

Arch4221: UEFI Secure Boot

TC3211: Intel Boot Guard

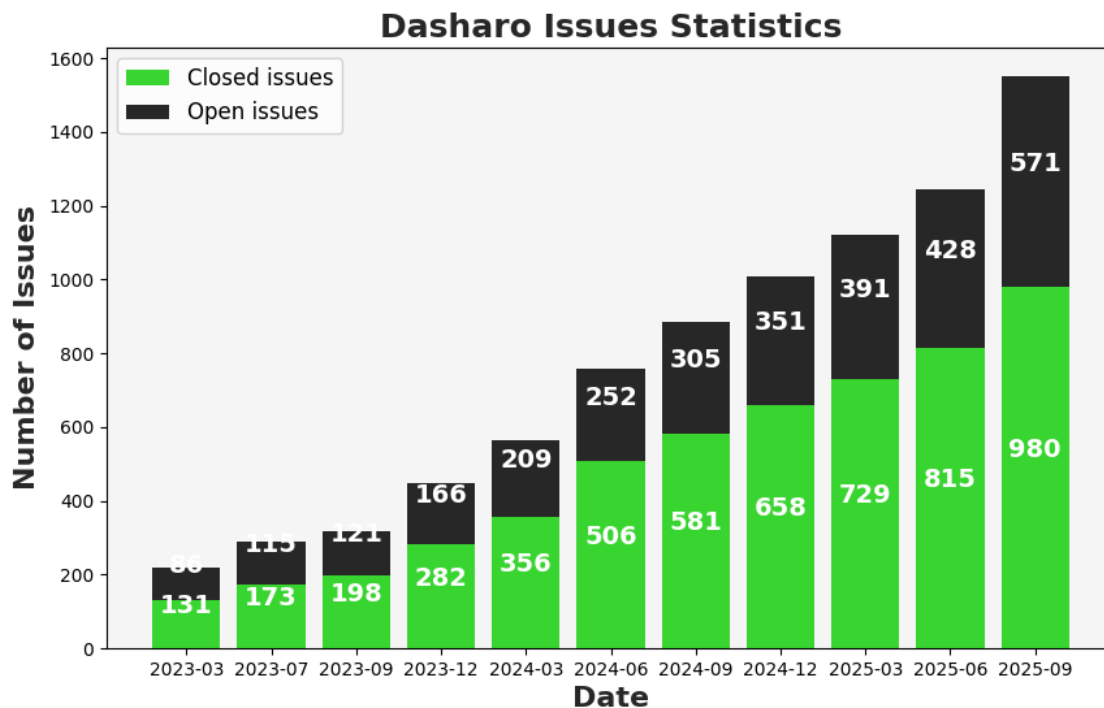
Dasharo Issues



1551 (+308)



980 (+165)



Dasharo Issues

Comments

 **7275 (+834)**  **170 (+9)**

Top Contributors



- **wessel-novacustom (471)**
- **tlaurion (196)**
- **zirblazer (150)**
- **renehoj (84)**
- **marmarek (79)**
- **Firminator (54)**

Dasharo/coreboot PRs



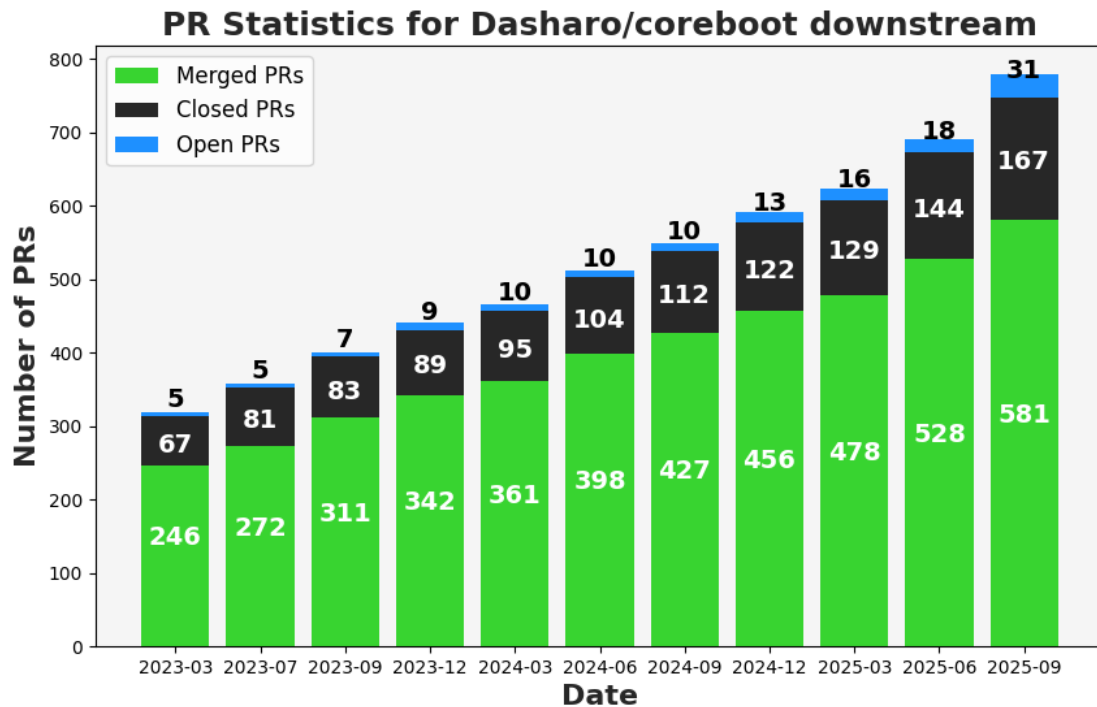
690 (+62)



508 (+31)

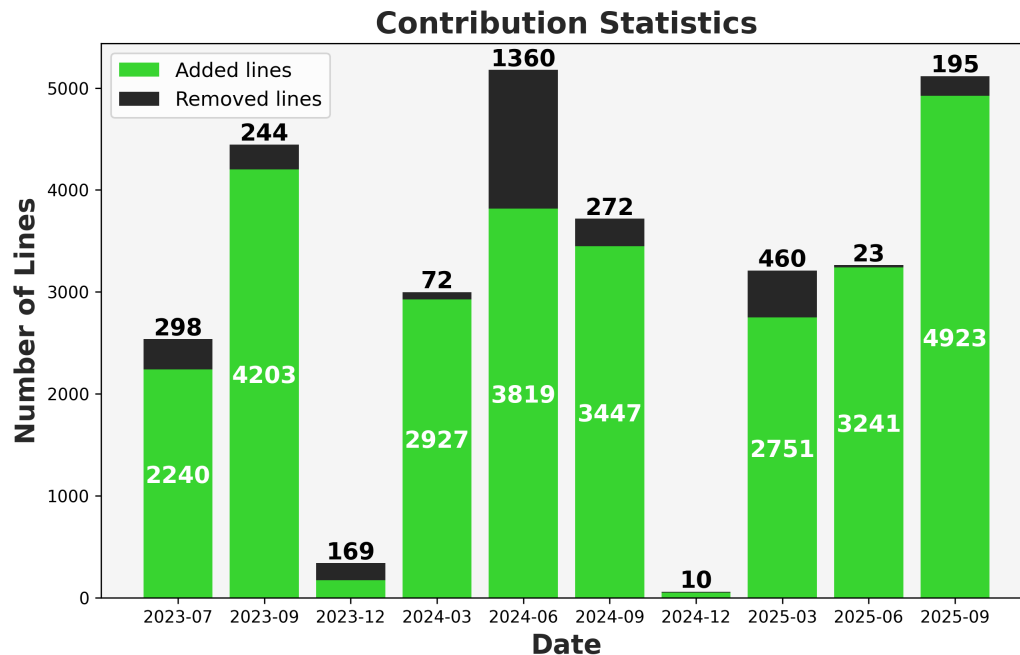


152 (+22)



Dasharo/coreboot upstreaming

  +58962 (+4923) / -43858 (-195)



Delta dasharo branch vs upstream v24.12 tag

673 files changed, 2237 insertions(+), 40101 deletions(-)

Top Upstreamers

- Michał Żygowski (miczyg): +2511/-48
 - *src/superio/nuvoton: Add HWM initialization code*
 - *mb/msi/{ms7d25,ms7e06}/devicetree.cb: Add fan control config*
 - *util/amdfwtool: Handle address mode properly for Turin*
- Michał Kopeć (mkc): +1071/-4
 - *mb/novacustom/mtl-h/var/dgpu: Add NVIDIA dGPU ASL code*
 - *mb/lenovo/m900_tiny: Put options in CFR cbtable*
- Krystian Hebel: +793/-58
 - *soc/power9/rom_media.c: find CBFS in PNOR*
 - *ppc64: Kconfig switch for bootblock in SEEPROM, zero HRMOR*

Dasharo TrustRoot

Users willing to achieve highest level of security hardening can take advantage of **Dasharo TrustRoot**. It's available on MeteorLake (MTL) devices since v1.0.0 release. This is done by choosing a fused version of binaries via **DTS**. Capsule updates never enable this feature.



Warning

This feature cannot be disabled after being enabled on a given hardware. Switching it on constrains all future firmware updates. See **Dasharo TrustRoot** for more details.

<https://docs.dasharo.com/unified/novacustom/features/#dasharo-trustroot>

PCR measurements performed by Dasharo firmware



Introduction

As part of measured boot process firmware hashes (measures) various pieces of code or data and updates PCRs of a TPM device. This allows a user (typically, automatically) to attest integrity of the system by verifying PCR values after a boot or tying decryption of data to expected values.

Usually the firmware is not the only entity which updates PCRs and even if it is, the number of updates can be large, so it's important to know which values do get measured to which PCRs and under what conditions (e.g., some measurements are done in response to user actions).

TPM event log maintained throughout the boot process is meant to track this kind of information, but due to limitations of its format the log is rarely enough to understand all of the measurements. This document is meant to describe when Dasharo updates PCRs so users would know which PCRs to use for sealing secrets and when to expect their values to be changed.

Firmware components are described separately because not all components might be present in a given firmware variant.

<https://docs.dasharo.com/kb/pcr-measurements/>

Sovereign Boot Provisioning Wizard



Introduction and motivation

Sovereign Boot Provisioning Wizard is an UEFI application designed to guide end users through the provisioning of UEFI Secure Boot. The objective is to offer a user-controllable mechanism for managing platform trust relationships and establishing UEFI Secure Boot infrastructure, with a primary focus on transparency, informed consent, and usability.

Unlike traditional firmware interfaces, which expose UEFI Secure Boot as a collection of loosely connected toggleable settings and unmanaged certificate stores, this application presents a coherent, wizard-like experience. Its purpose is to make the process of reviewing and enrolling platform keys intuitive for users who are not security experts.

Specification

The application is implemented based on the [Sovereign Boot Provisioning Wizard Specification](#) (current revision v0.1.0).

Credits

This research has been supported by [Power Up Privacy](#), a privacy advocacy group that seeks to supercharge privacy projects with resources so they can complete their mission of making our world a better place.

<https://docs.dasharo.com/projects/sovereign-boot-wizard/>

Dasharo/edk2 PRs



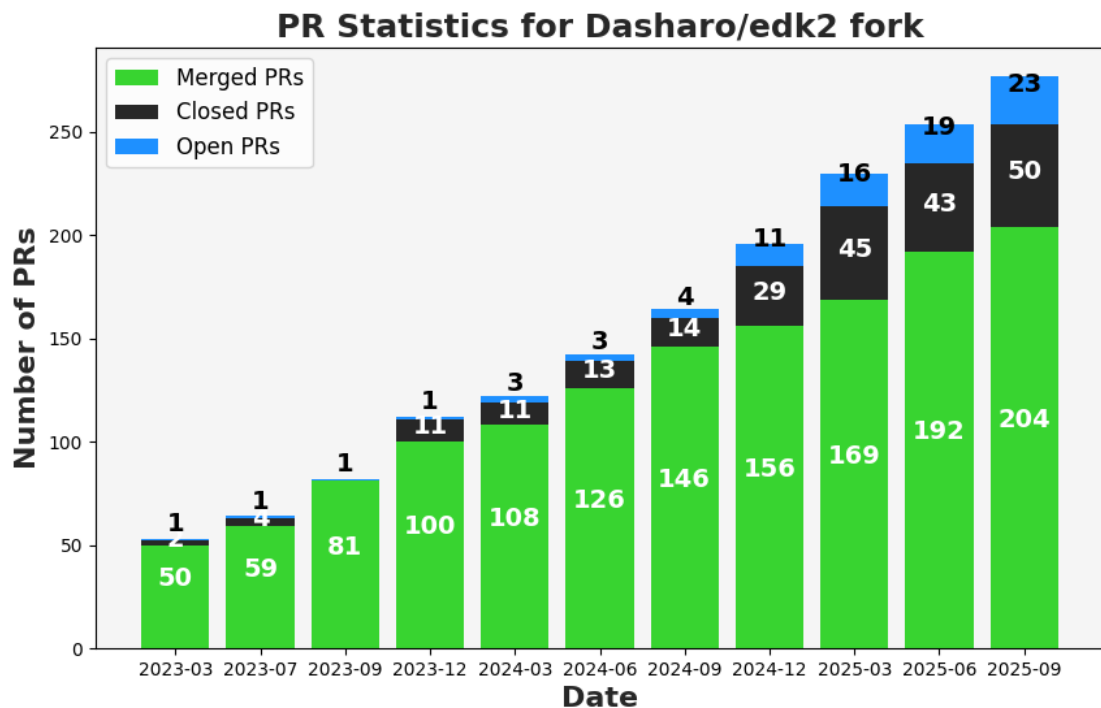
277 (+23)



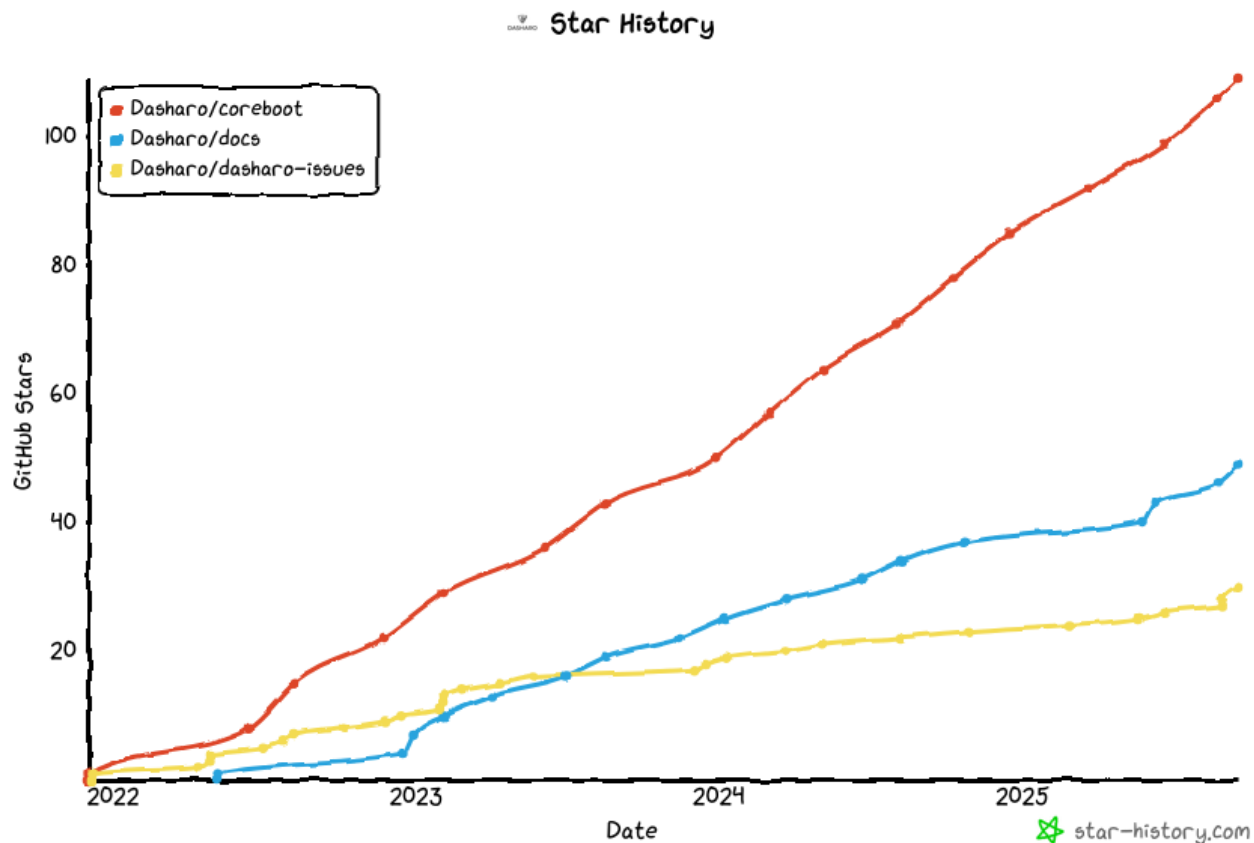
204 (+12)



50 (+7)



Dasharo star history



Dasharo Matrix Community

Messages and Users

 **38k (+2k)**  **458 (+28)**

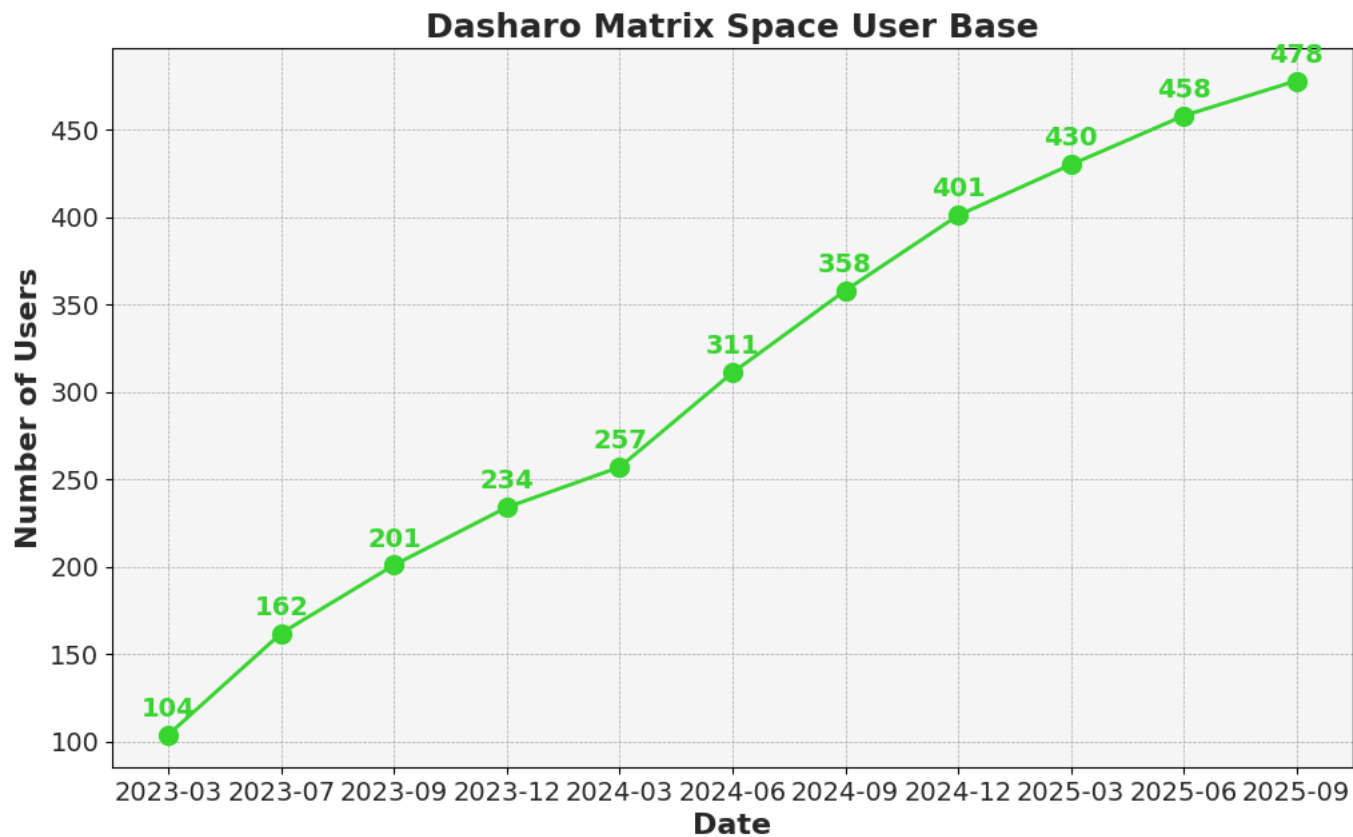
Top contributors



- **zir-blazer** (8709)
- **collector-yhn** (1314)
- **hanetzer** (1079)
- **tlaurion** (827)
- **xutaxkamay** (714)

Top Contributors Benefits

- Unlimited access to the Dasharo Pro Package
- Up to 15% discount on hardware sold by 3mdeb (excluding dropshipping)
- How to claim?
 - Write an email to: contact@dasharo.com



Most active Dasharo Community Matrix channels since last DUG

Random (`#dasharo-random:matrix.org`)

Support (`#dasharo-support:matrix.org`)

Laptops (`#dasharo-laptops:matrix.org`)

is:issue state:open label:bounty

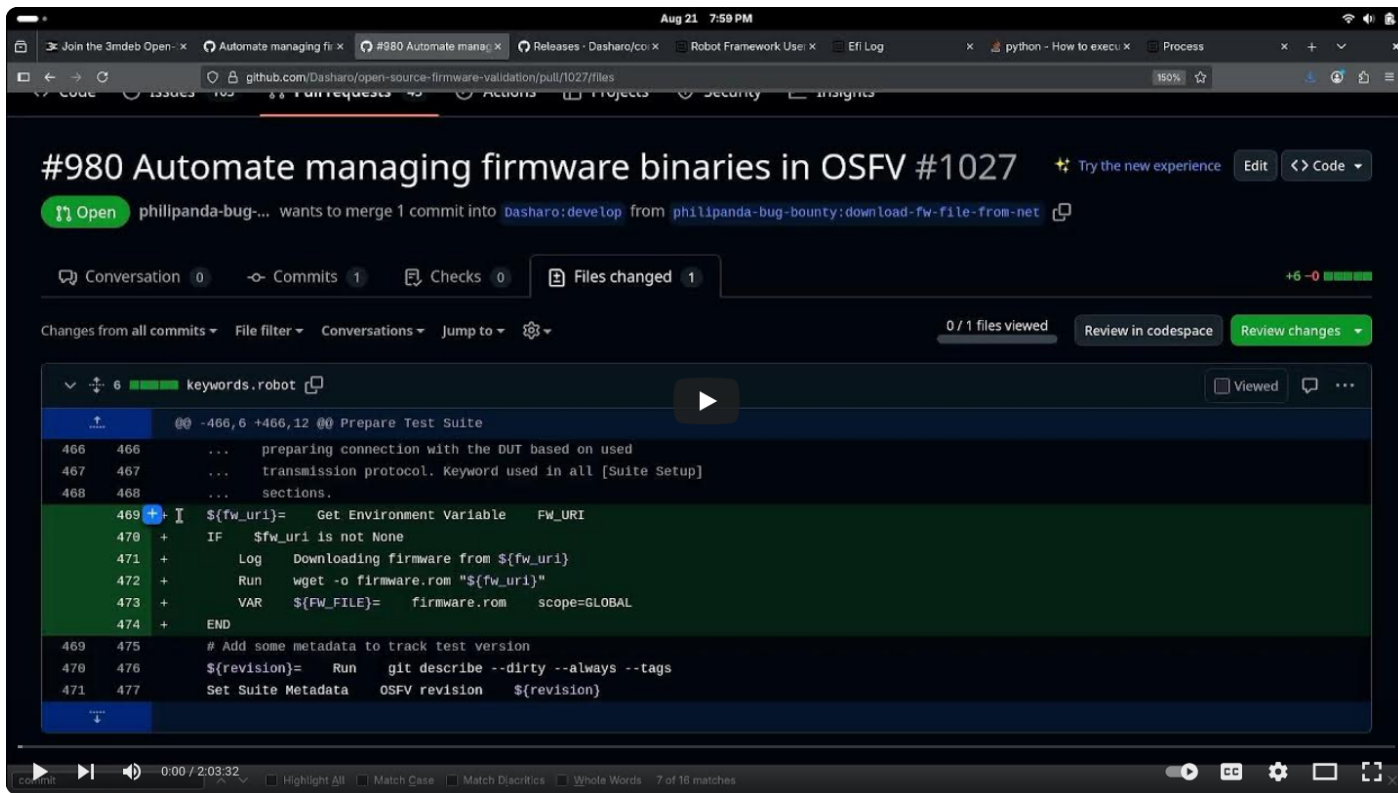
Labels Milestones New issue

Open 11 Closed 6

Author Labels Projects Milestones Assignees Types Newest

- DTS supported platforms and workflows generation** bounty bounty-easy DasharoToolsSuite doc documentation enhancement 3
- Duplicated message asking for sending logs in DTS, e.g.:** bounty bounty-warmup bug DasharoToolsSuite needs review
- DTS: Entering empty password results in UI bugs** bounty bounty-warmup bug DasharoToolsSuite DasharoToolsSuiteUI good first issue 6
- Replace ipxe menu with Dasharo network boot menu** bounty bounty-warmup enhancement good first issue pcengines_apu2
- EC testability interface** bounty bounty-hard EC enhancement novacustom_ns5x7x_adl novacustom_ns5x7x_tgl novacustom_ns7x_tgl novacustom_nv4x_adl novacustom_nv4x_tgl novacustom_v54_mtl novacustom_v56_mtl 4
- DTS: R to reboot and P to poweroff don't work over SSH** bounty bounty-easy bug DasharoToolsSuite MSI PRO Z690-A boards MSI PRO Z790-P boards 1
- Implement an "Unobtrusive Mode" for Dasharo coreboot** bounty bounty-medium enhancement novacustom_ns5x7x_adl novacustom_ns5x7x_tgl novacustom_nv4x_adl novacustom_nv4x_tgl novacustom_v54_mtl novacustom_v56_mtl 8

[https://github.com/Dasharo/dasharo-issues/issues?q=is%3Aissue
state%3Aopen label%3Abounty](https://github.com/Dasharo/dasharo-issues/issues?q=is%3Aissue%3Aopen%3Alabel%3Abounty)



<https://www.youtube.com/live/aFhYhzQgy8Y>

The image features a dark gray background with the word "Questions?" centered in a bright green, sans-serif font. In the corners, there are decorative elements resembling circuit board traces or stylized lines. These lines are light gray and form various geometric shapes, including straight lines, right angles, and small circles at the ends, suggesting a technological or digital theme.

Questions?