👋 Dasharo User Group #11 🎉 and Developers vPub 0x10 🍻

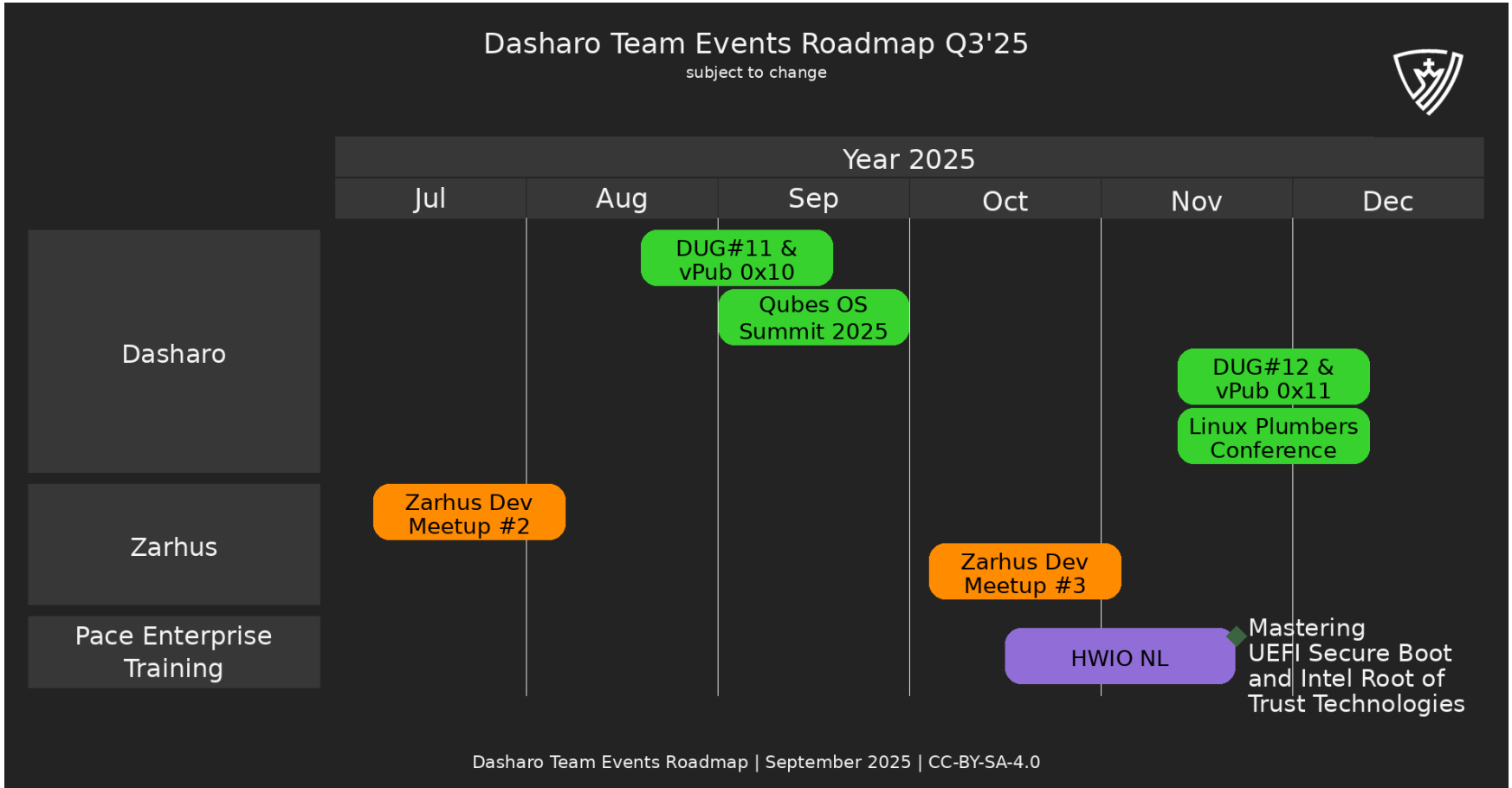
👋 Dasharo User Group #11 🎉

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

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0



© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the 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

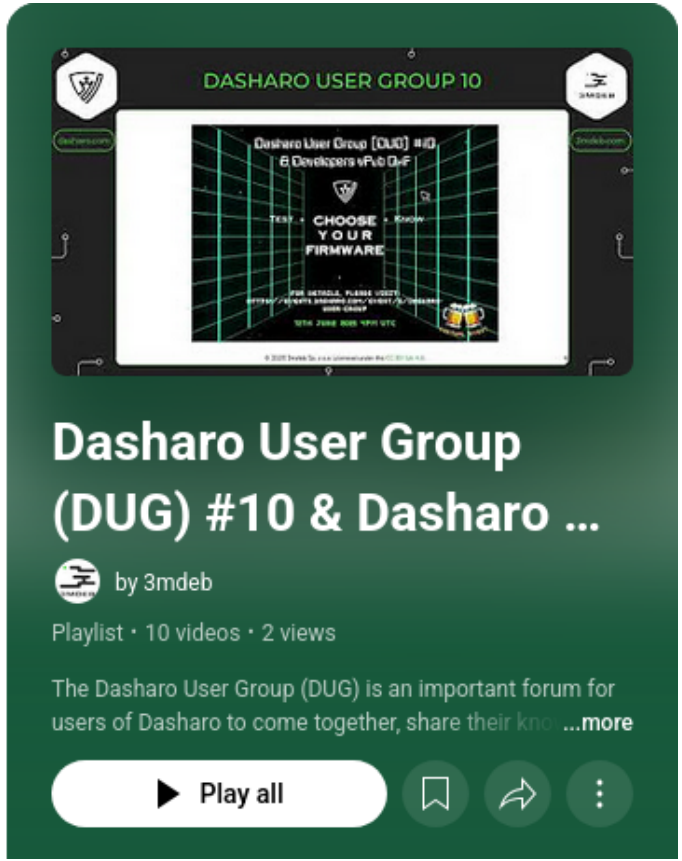
- Bug Bounty Program **Live Demo**
- Zarhus **Developers Meetup 2**
- Dasharo User Group 10 **& Developers vPub 0xF**
- Zarhus **Developers Meetup 1**
- Dasharo User Group 9 **& Developers vPub 0xE**
- FOSDEM **2025**
- Xen Project **Winter Meetup**

2021

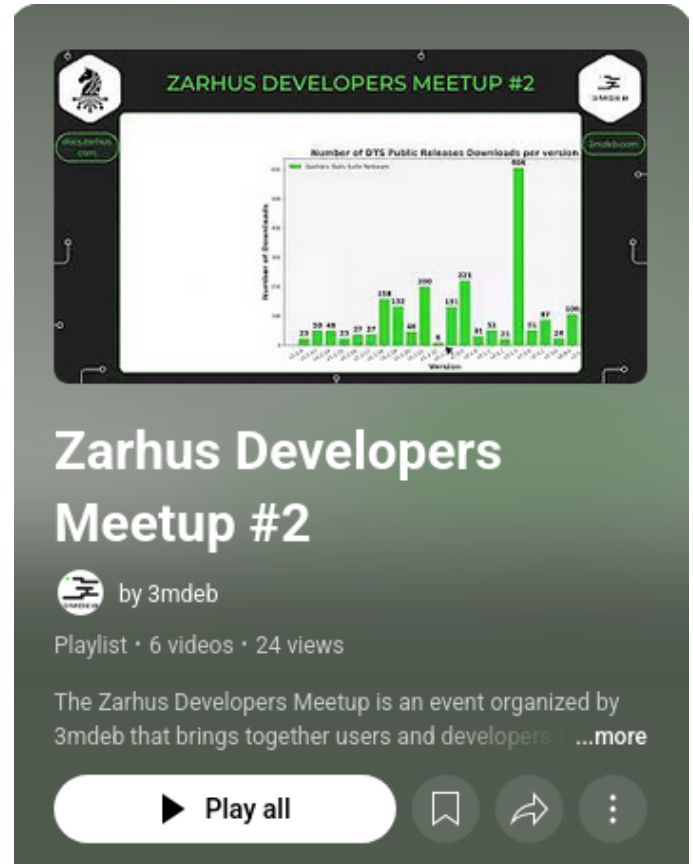
- Yocto Project **Virtual Summit**
- Dasharo OSF vPub Fall 2021 **(aka 3mdeb vPub vol. 3)**
- Linux Secure Launch - **TrenchBoot Summit**
- OpenPOWER **Summit**
- TPM.dev **2021 MiniConf**
- Linux Plumbers **Conference**
- Euro**BSDCon**
- Qubes OS **Minisummit**
- OpenPOWER **Community Call**
- Zephyr 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

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0



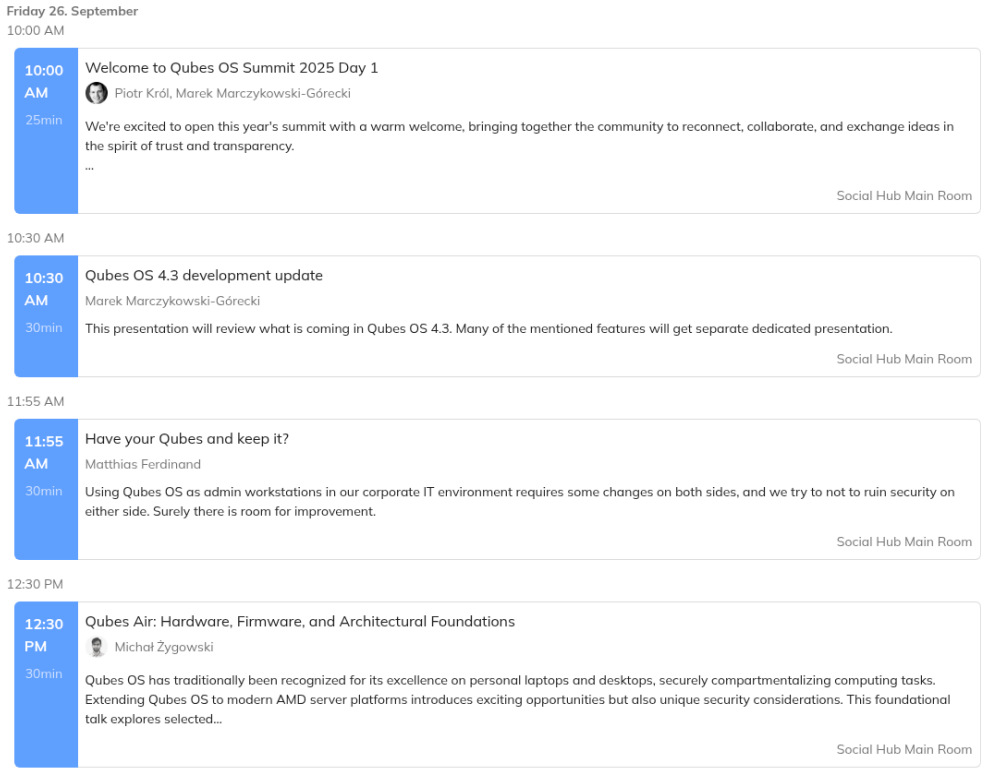
Link to DUG#10 and vPub 0xF YouTube playlist and slides.



Link to ZDM#2 YouTube playlist and slides.

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0



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

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

2:30 PM

2:30 PM (30min)

Rethinking the compartmentalization experience

Alyssa Ross

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 (30min)

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

Piotr Król

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 (30min)

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

Ali Mirjamali

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 (60min)

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

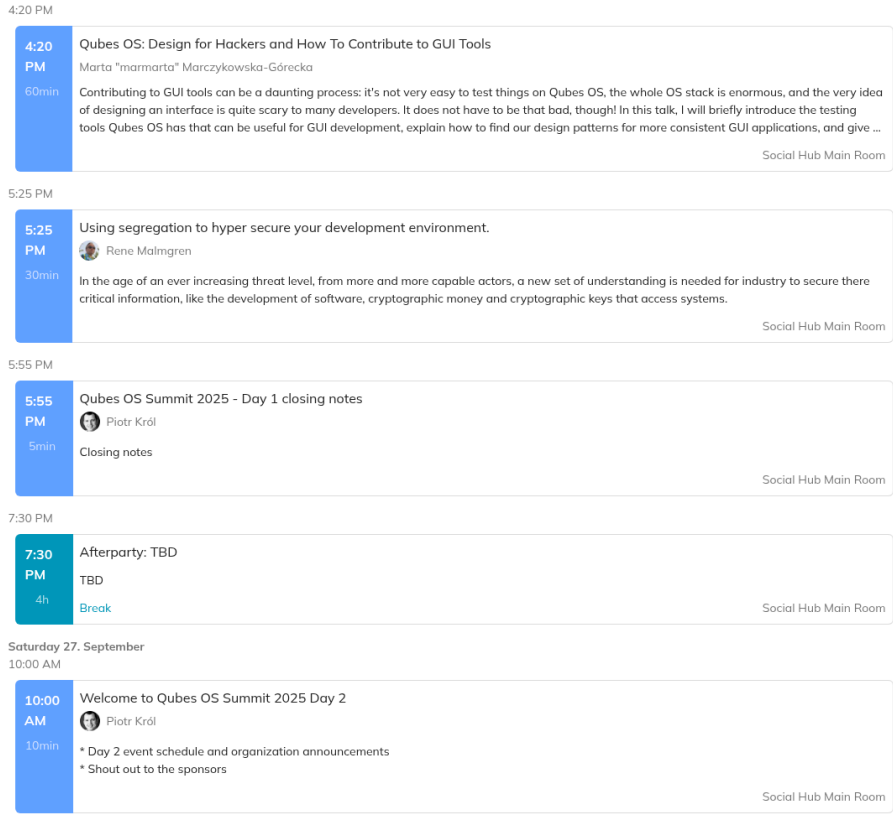
Marta "marmarta" Marczykowska-Górecka

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

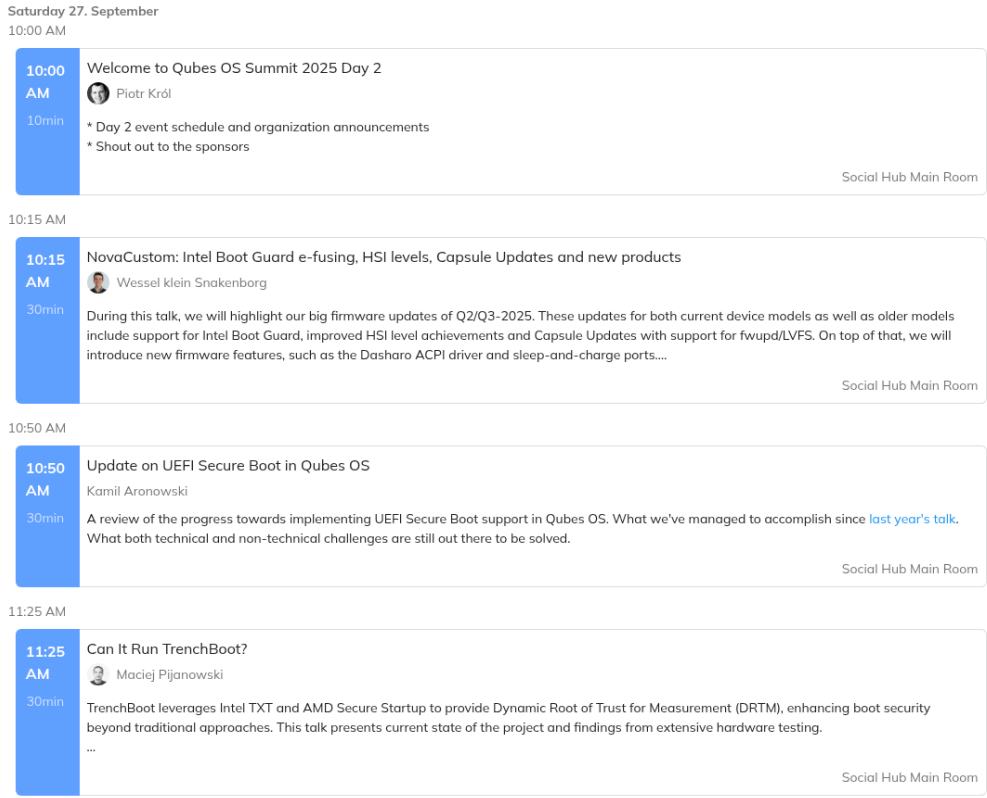
https://events.dasharo.com/event/2/qubes-os-summit-2025

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0



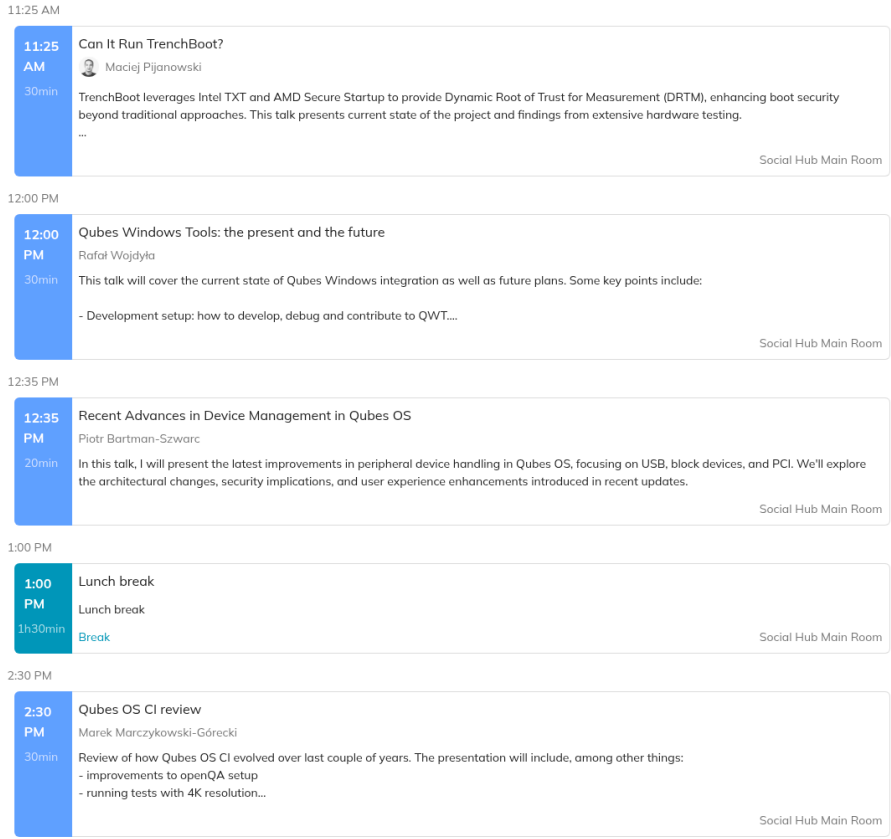
https://events.dasharo.com/event/2/qubes-os-summit-2025

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0



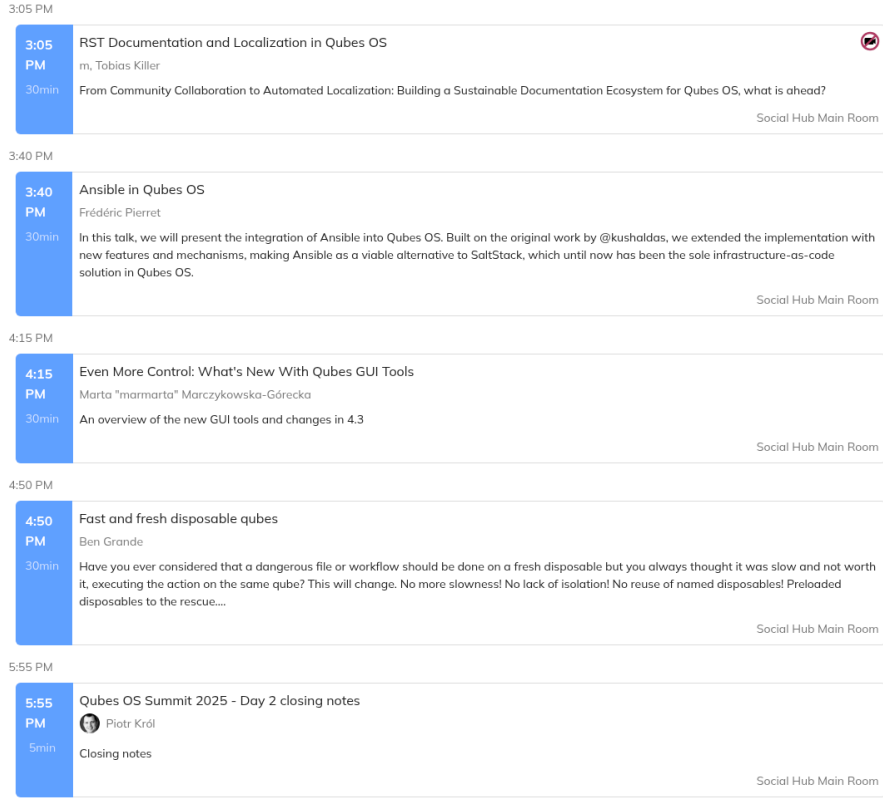
https://events.dasharo.com/event/2/qubes-os-summit-2025

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0



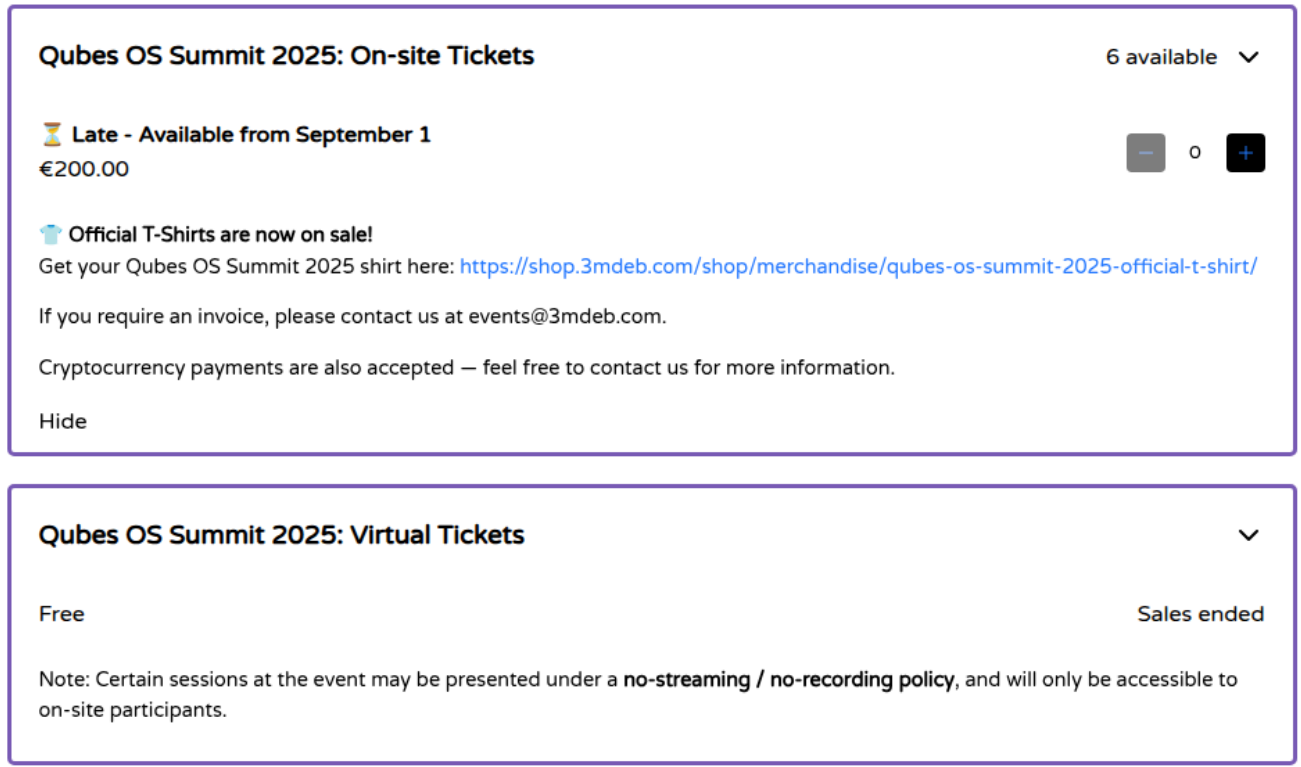
https://events.dasharo.com/event/2/qubes-os-summit-2025

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0



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

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

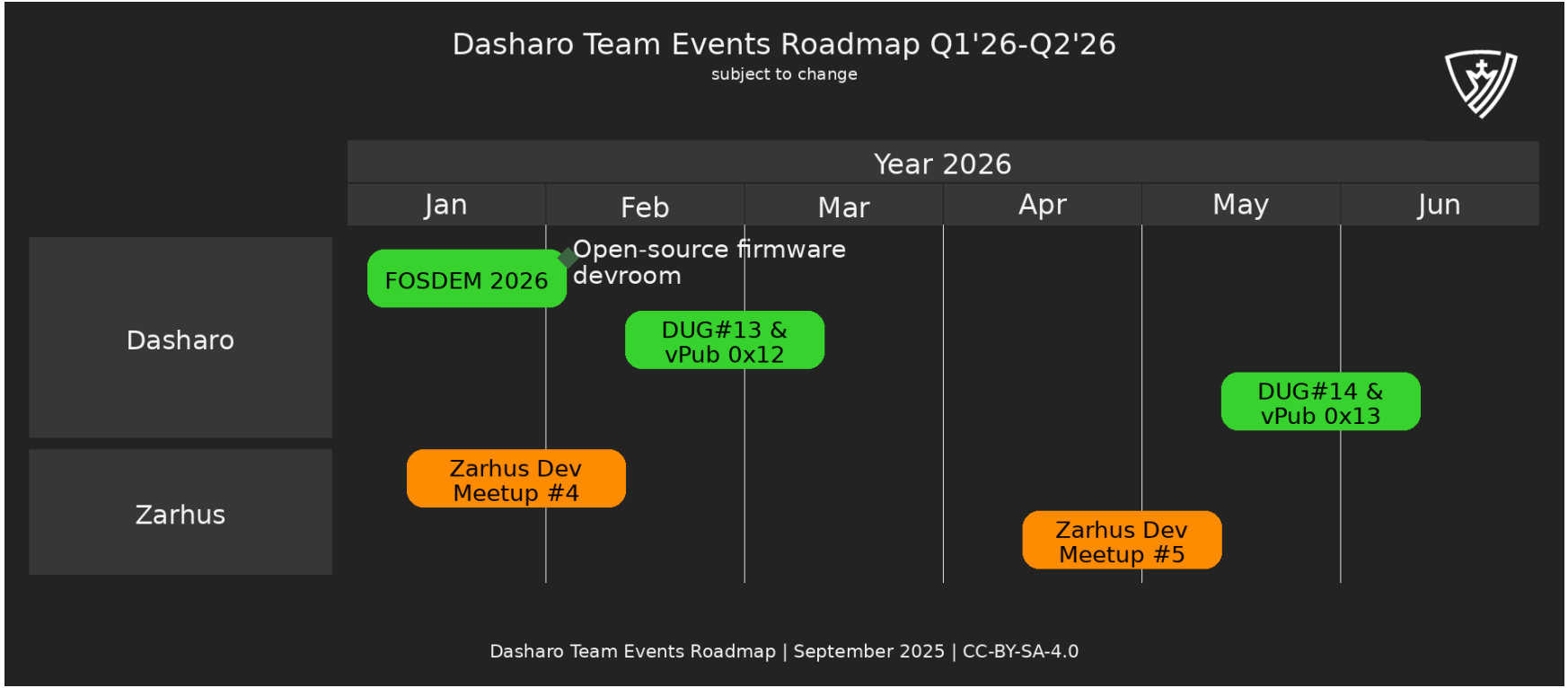


https://events.dasharo.com/event/2/qubes-os-summit-2025

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

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

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0



© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

Use QR code to get news about upcoming OST2 classes:

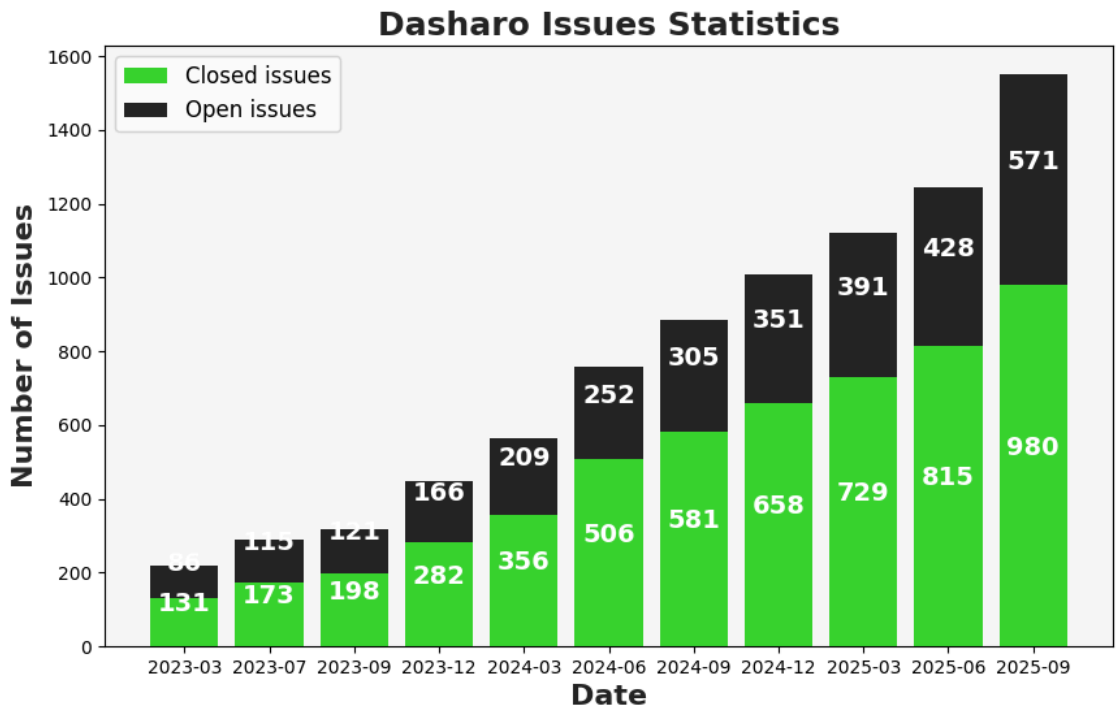
Arch4221: UEFI Secure Boot

TC3211: Intel Boot Guard

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

Dasharo Issues

1551 (+308) 980 (+165)



© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

Dasharo Issues

Comments

 7275 (+834)  170 (+9)

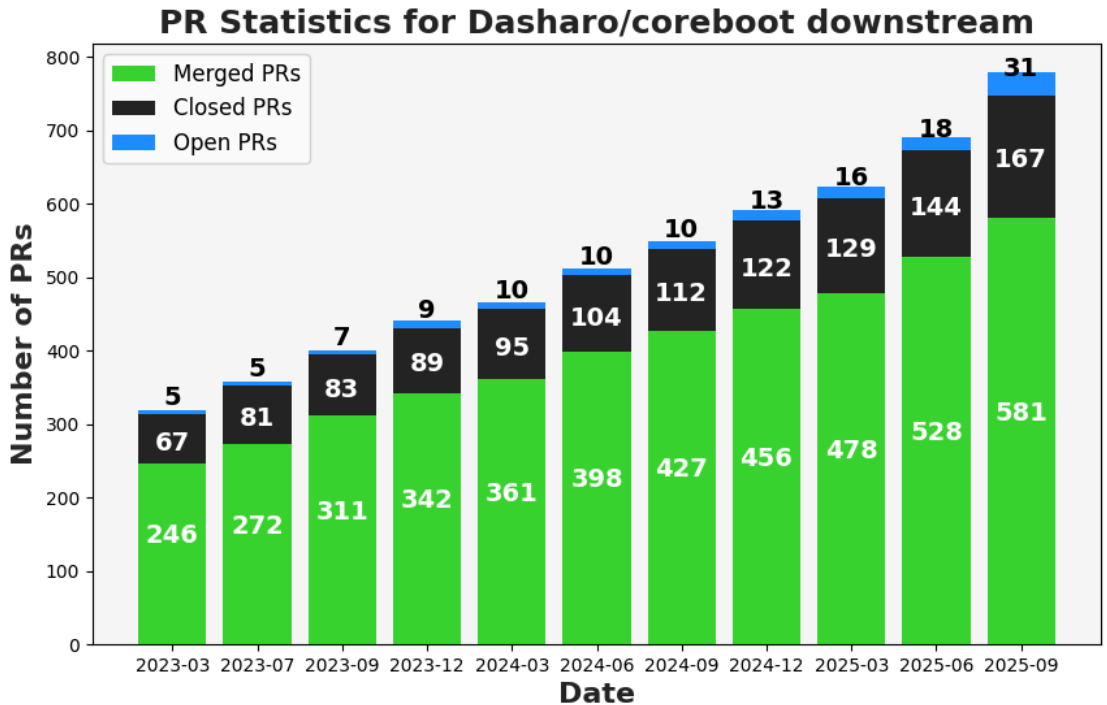
Top Contributors

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

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

Dasharo/coreboot PRs

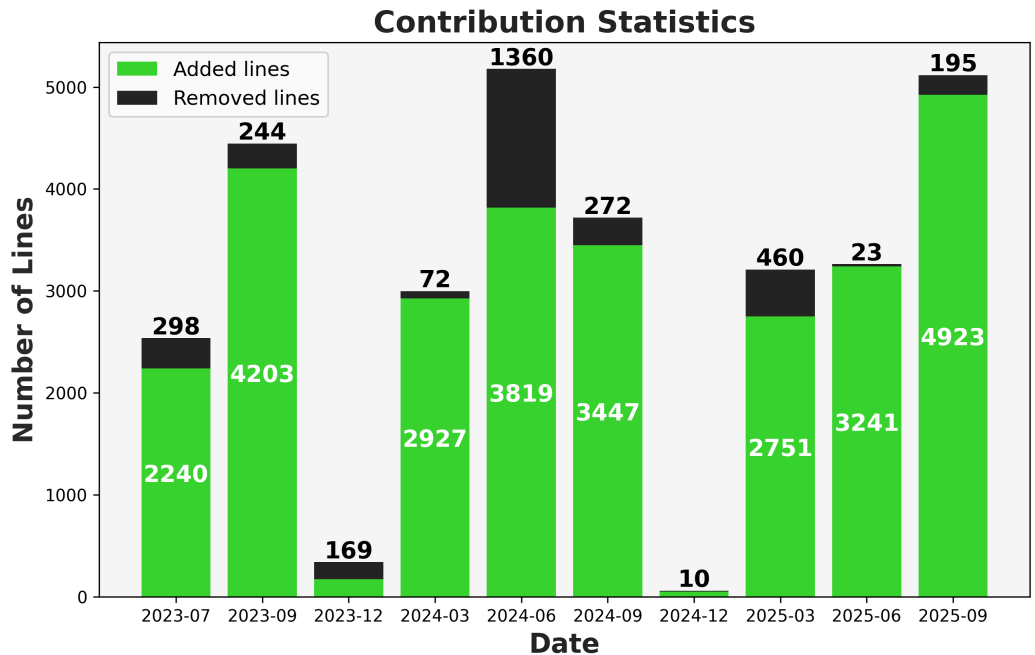
690 (+62) 508 (+31) 152 (+22)



© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

Dasharo/coreboot upstreaming

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



© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

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*

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

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

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

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/

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

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

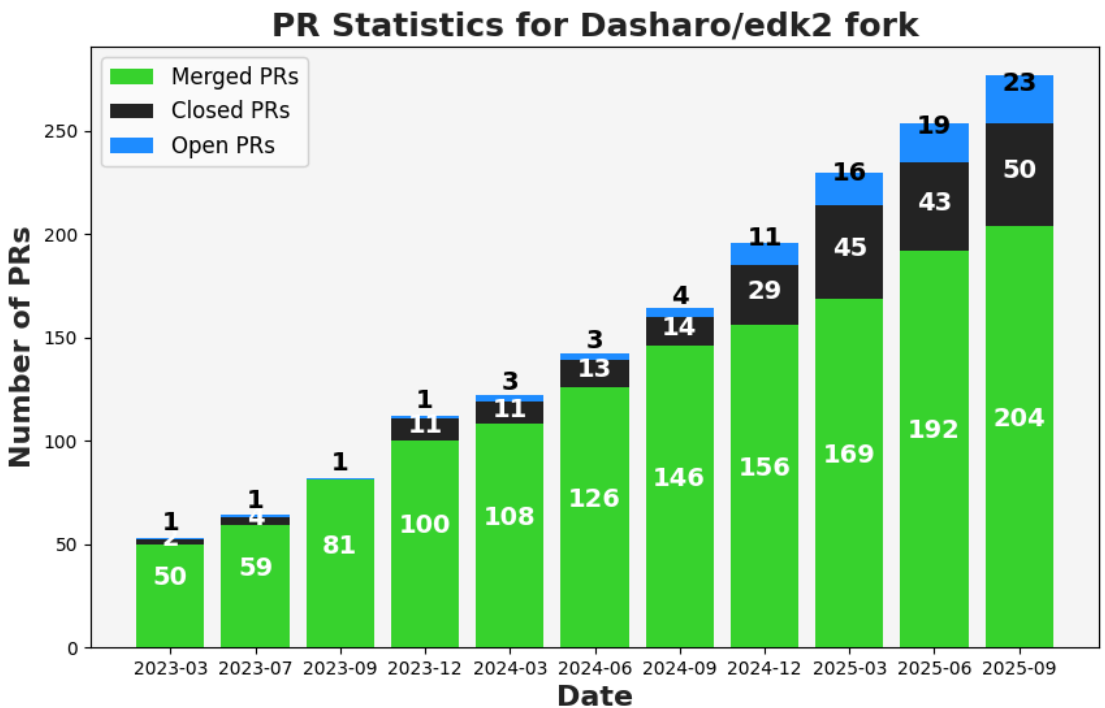
This research has been supported by Power Up Privacy, a privacy advocacy group that seeks to supercharge privacy projects with resources so they can complete their mission of making our world a better place.

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

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

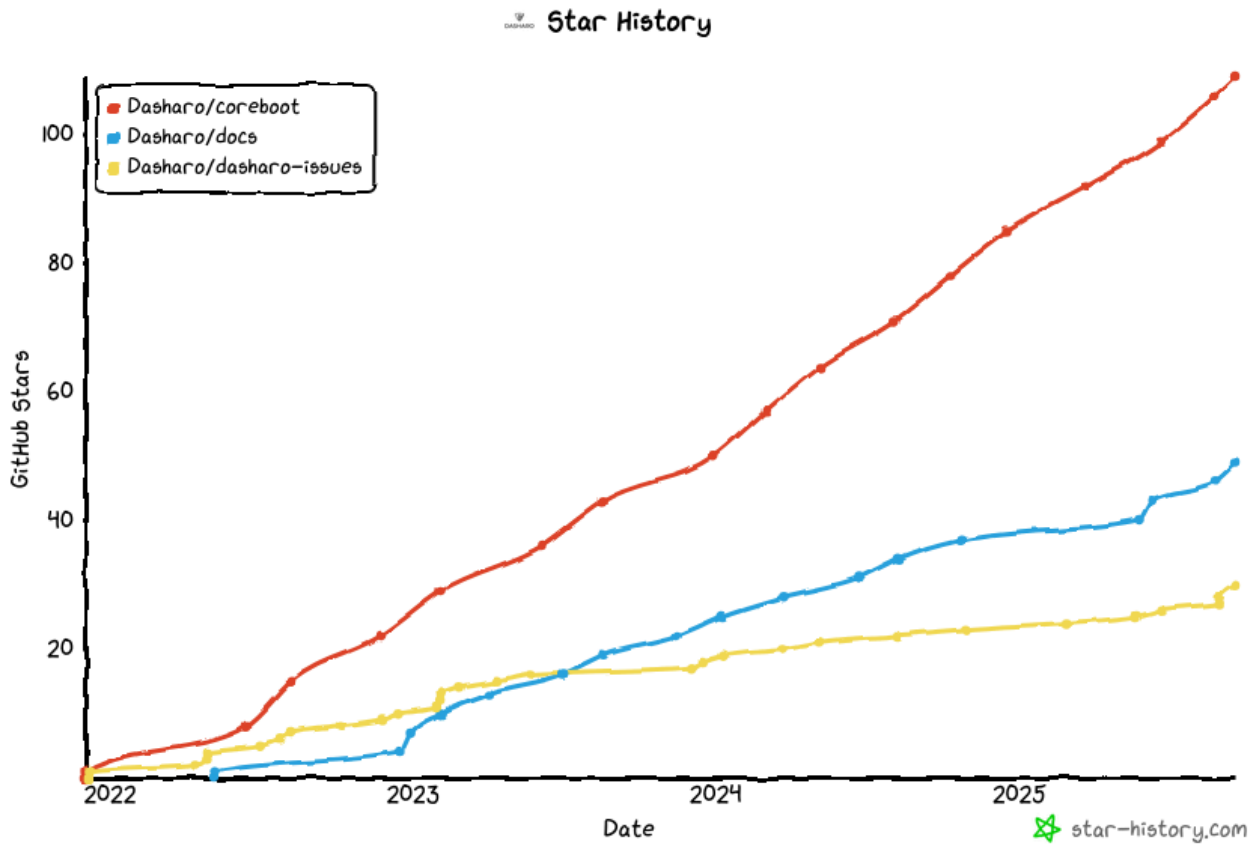
Dasharo/edk2 PRs

277 (+23) 204 (+12) 50 (+7)



© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

Dasharo star history



© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

Dasharo Matrix Community

Messages and Users

38k (+2k)

458 (+28)

Top contributors

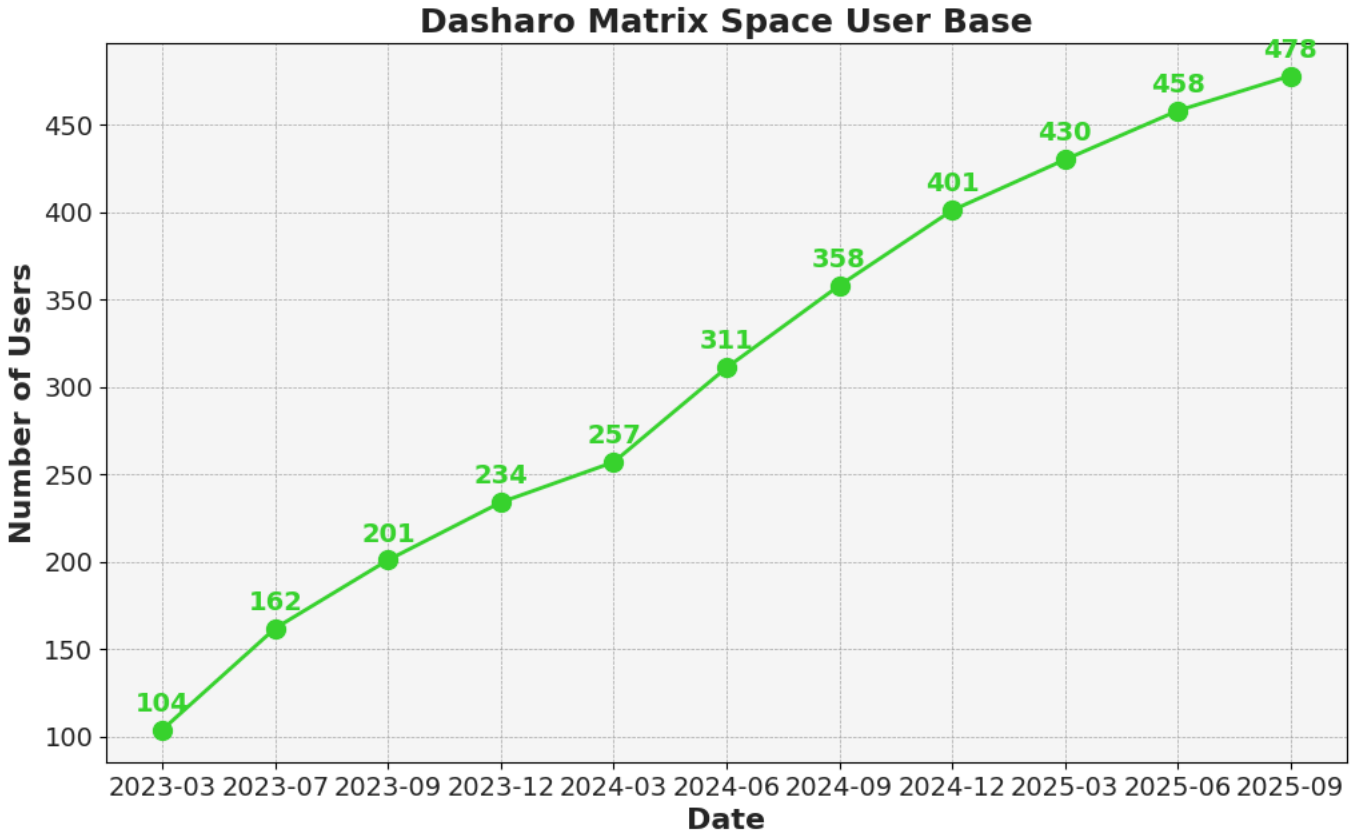
- **zir-blazer (8709)**
- **collector-yhn (1314)**
- **hanetzer (1079)**
- **tlaurion (827)**
- **xutaxkamay (714)**

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

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

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0



© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

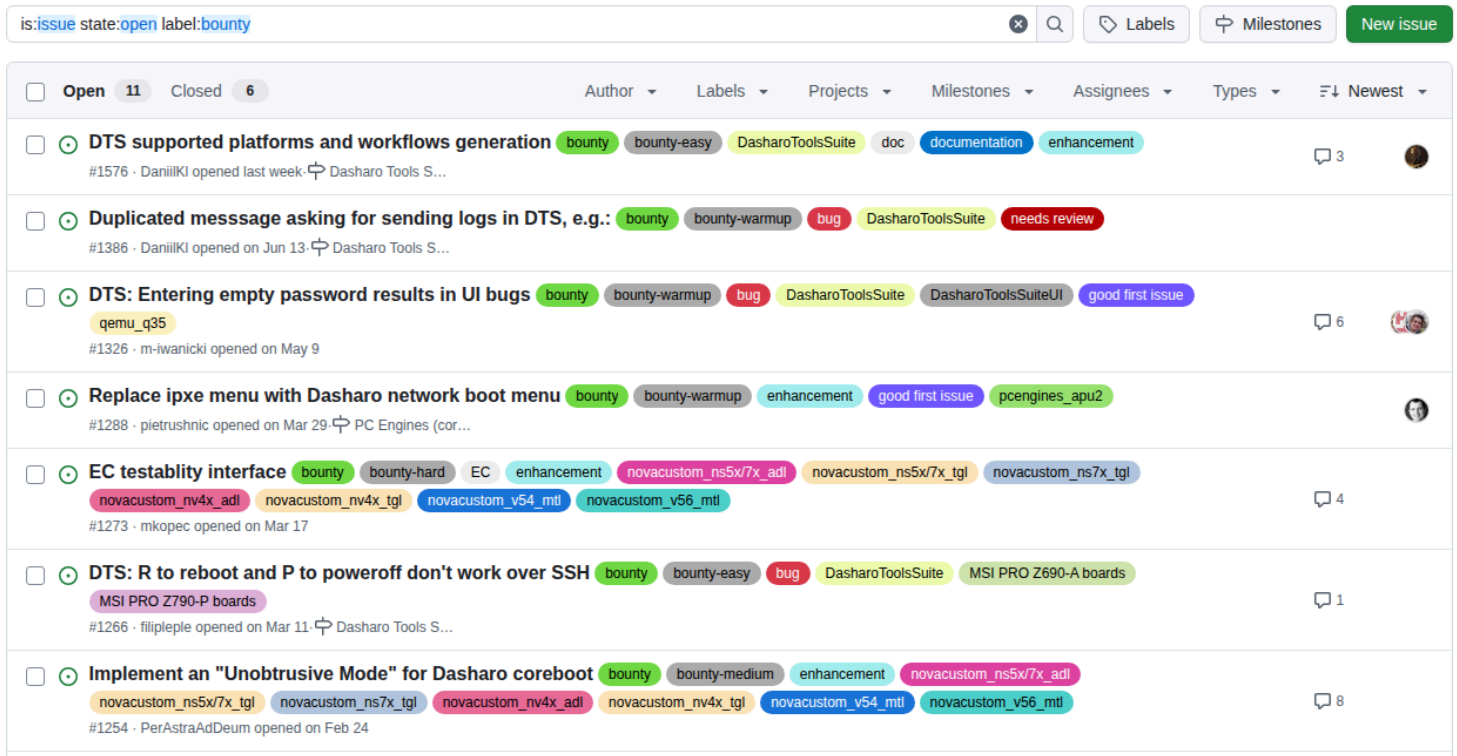
Most active Dasharo Community Matrix channels since last DUG

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

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

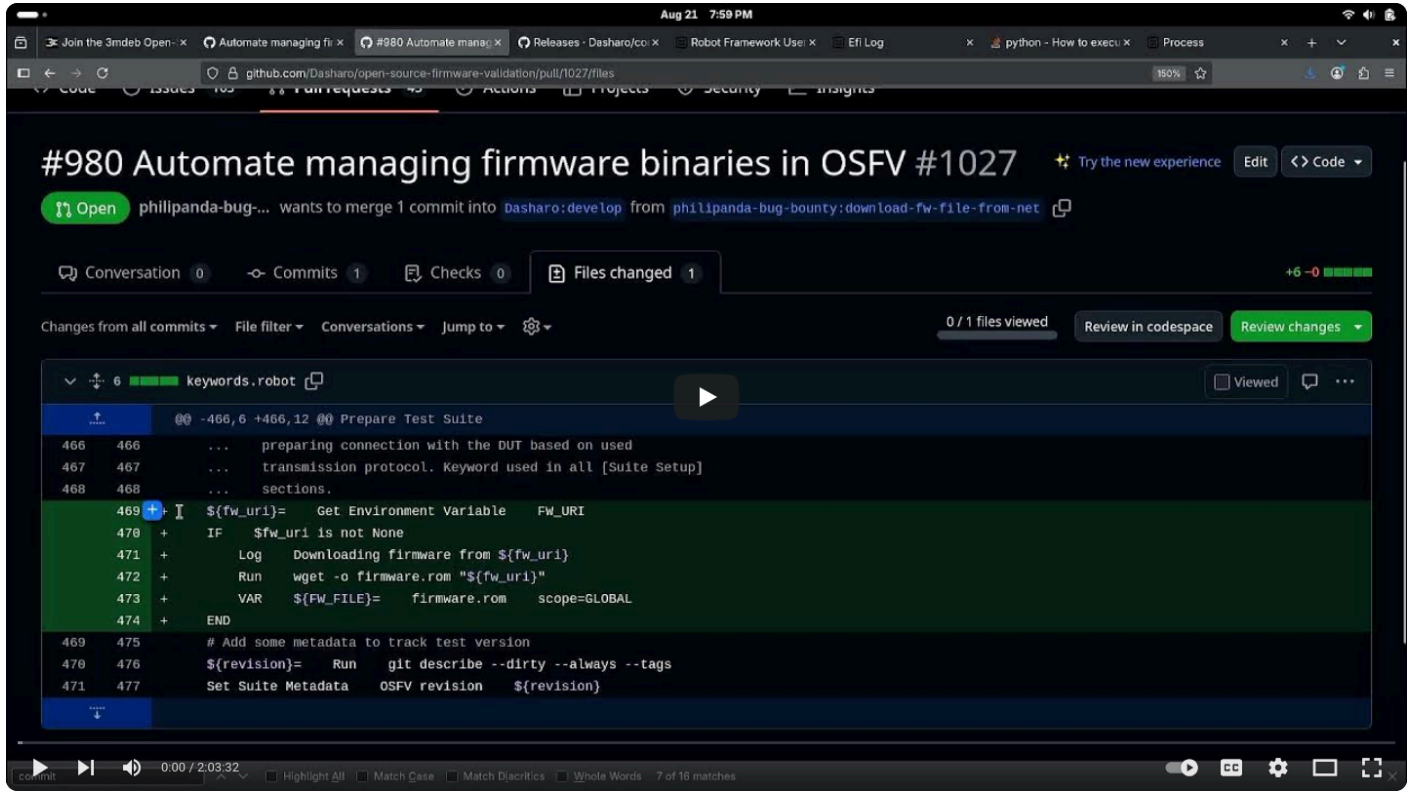
Laptops (`#dasharo-laptops:matrix.org`)

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0



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

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0



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

© Copyright 2025. 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0

Questions?