Content

1. What happened during last two years
2. Coverity - x86_64/EFI and ARM64/EFI runs - 0 outstanding defects
3. What is happening in the GRUB project now
4. Fedora downstream GRUB patches - rough estimates
What happened during last two years

• GRUB 2.12 release which contains
  • GCC 13 support
  • clang 14 support
  • binutils 2.38 support
  • Unification of EFI Linux kernel loader across architectures
  • Transition to EFI Linux kernel stub loader for x86 architecture
  • Initial support for Boot Loader Interface (bli module)
  • Support for dynamic GRUB runtime memory addition using firmware calls
  • PCI and MMIO UARTs support
  • SDL2 support
  • LoongArch support
  • TPM driver fixes
  • Many filesystems fixes
  • Many CVE and Coverity fixes
  • Debugging support improvements
  • Tests improvements
  • Documentation improvements
  • ... and tons of other fixes and cleanups...
Andrei Borzenkov started Coverity work in 2014
Later Vladimir Serbinenko joined and together continued this work until 2017
Covertiy work was restarted in 2020, when we were fixing BootHole security vulnerability and other issues
It took us 3 years to do analysis of all Coverity issues not solved earlier
We did analysis of 629 issues and fixed 535 of them
New Coverity tool revealed 4 additional issues in December 2023
All of them are fixed right now
Now in general we will not accept patches which contain issues reported by the Coverity
We are also employing fuzzing and other tools to find bugs in GRUB code
Big thank you for folks who were doing this work:
  • Alec Brown (Oracle)
  • Alexey Makhalov (VMware)
  • Andrei Borzenkov
  • Chris Coulson (Canonical)
  • Daniel Axtens
  • Darren Kenny (Oracle)
  • Glenn Washburn
  • Jagannathan Raman (Oracle)
  • Jan Setje-Eilers (Oracle)
  • Konrad Rzeszutek Wilk (Oracle)
  • Marco A Benatto (Red Hat)
  • Patrick Steinhardt
  • Paulo Flabiano Smorigo (Canonical)
  • Ross Philipson (Oracle)
  • Vladimir Serbinenko
  • WANG Xuerui
What is happening in the GRUB project now

- NX support for EFI platforms
  - *Section Alignment of the submitted PE file must be aligned with page size. This must be 4kb, or a larger power of 2 (ex 64kb)*
  - *Section Flags must not combine IMAGE_SCN_MEM_WRITE and IMAGE_SCN_MEM_EXECUTE for any given section.*
- TrenchBoot support for Intel and AMD x86 architectures
- Update embedded libs to latest versions
- Libgcrypt update or replacement - required for Argon2 KDF
- Automatic Disk Unlock with TPM2
- Forward porting downstream patches to upstream
- Fixes, cleanups and documentation updates…
- Setup CI infrastructure
- Next code freeze around October 2024
- Next GRUB release around November 2024

https://techcommunity.microsoft.com/t5/hardware-dev-center/updated-uefi-signing-requirements/ba-p/1062916
Fedora downstream GRUB patches - rough estimates
Stats prepared by Alec Brown from Oracle

GRUB 2.02

- Fedora 21 has 151 patches, 87 patches were backported, 64 new patches, total 64
- Fedora 22 has 162 patches, 89 patches were backported, 9 new patches, total 73
- Fedora 23 has 77 patches, 1 patch was backported, 7 new patches, total 80
- Fedora 24 has 97 patches, 2 patches were backported, 32 new patches, total 112
- Fedora 25 has 97 patches, 2 patches were backported, 0 new patches, total 112
- Fedora 26 has 107 patches, 3 patches were backported, 10 new patches, total 122
- Fedora 27 has 135 patches, 6 patches were backported, 28 new patches, total 150
- Fedora 28 has 219 patches, 3 patches were backported, 110 new patches, total 260
- Fedora 29 has 244 patches, 3 patches were backported, 24 new patches, total 284
- Fedora 30 has 300 patches, 3 patches were backported, 58 new patches, total 342
- Fedora 31 has 237 patches, 30 patches were backported, 28 new patches, total 370
Fedora downstream GRUB patches - rough estimates

... continuation...

GRUB 2.04
- Fedora 32 has 250 patches, 28 patches were backported, 25 new patches, total 395
- Fedora 33 has 196 patches, 0 patches were backported, 42 new patches, total 437

GRUB 2.06
- Fedora 34 has 222 patches, 3 patches were backported, 23 new patches, total 460
- Fedora 35 has 283 patches, 45 patches were backported, 19 new patches, total 479
- Fedora 36 has 296 patches, 48 patches were backported, 40 new patches, total 519
- Fedora 37 has 331 patches, 79 patches were backported, 13 new patches, total 532
- Fedora 38 has 347 patches, 84 patches were backported, 11 new patches, total 543
- Fedora 39 has 348 patches, 84 patches were backported, 1 new patch, total 544
- Fedora 40 has 348 patches, 84 patches were backported, 0 new patches, total 544
Thank you

Daniel Kiper
daniel.kiper@oracle.com