[SECURITY PATCH 0/8] GRUB2 vulnerabilities - 2025/11/18

From: Daniel Kiper

Subject: [SECURITY PATCH 0/8] GRUB2 vulnerabilities - 2025/11/18

Date: Tue, 18 Nov 2025 19:00:13 +0100

Hi all,

This patch set contains a bundle of fixes for various security flaws
discovered, as part of a pro-active hardening effort, in the GRUB2 code
recently. The most severe one, i.e. potentially exploitable, has CVE
assigned and is listed at the end of this email.

Details of exactly what needs updating will be provided by the respective
distros and vendors when updates become available.

Full mitigation against CVE will require updated shim with latest SBAT
(Secure Boot Advanced Targeting) [1] data provided by distros and vendors.
This time UEFI revocation list (dbx) will not be used and revocation of broken
artifacts will be done with SBAT only. For information on how to apply the
latest SBAT revocations, please see mokutil(1). Vendor shims may explicitly
permit known older boot artifacts to boot.

Updated GRUB2, shim and other boot artifacts from all the affected vendors will
be made available when the embargo lifts or some time thereafter.

I am posting all the GRUB2 upstream patches which fix all security bugs found
and reported up until now. Affected Linux distros carry or will carry soon one
form or another of these patches. Now all the GRUB2 upstream patches are in
the GRUB2 git repository [2] too.

I would like to thank Alec Brown, Jamie and Thomas Frauendorfer for responsible
disclosure and preparation of patches needed to fix known issues. Marco Benatto
has been helping with assigning CVEs and scores for the issues. Thank you!

Daniel

[1] https://github.com/rhboot/shim/blob/main/SBAT.md
    https://github.com/rhboot/shim/blob/main/Delivering_Sbat_Revocations.md

[2] https://git.savannah.gnu.org/gitweb/?p=grub.git
    https://git.savannah.gnu.org/git/grub.git

****

CVE-2025-54770: Missing unregister call for net_set_vlan command may lead to
use-after-free
CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L - 4.9

The net_set_vlan command is registered in the net module during load. However,
the command is not unregistered at the module unload. So, this may lead to
use-after-free issue when the net_set_vlan command is invoked after the

net module unload.

Reported-by: Thomas Frauendorfer

****

CVE-2025-54771: grub_file_close() does not properly controls the fs refcount
CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L - 4.9

When closing a file the grub_file_close() misses to dereference the filesystem
structure leading to possible invalid reference to the file->fs->mod pointer.
It may lead to a use-after-free vulnerability.

Reported-by: Thomas Frauendorfer

****

CVE-2025-61661: Out-of-bounds write in grub_usb_get_string() function
CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:H - 4.8

When reading strings from a USB device in grub_usb_get_string() function the
initial length is taken from first message read. Then this value is used to
allocate memory for UTF-8 destination string. However, during conversion the
length value is taken from the second USB device read. This can be dangerous
if malicious USB devices are connected because they may expose smaller initial
length value, used for memory allocation, and subsequent read may provide
larger length, used during conversion. Such behavior may lead to heap overflow
during UTF-16 to UTF-8 conversion.

Reported-by: Jamie

****

CVE-2025-61662: Missing unregister call for gettext command may lead to
use-after-free
CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L - 4.9

The gettext command is registered in the gettext module during load. However,
the command is not unregistered at the module unload. So, this may lead to
use-after-free issue when the gettext command is invoked after the gettext
module unload.

Reported-by: Alec Brown

****

CVE-2025-61663: Missing unregister call for normal commands may lead to
use-after-free
CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L - 4.9

The normal command is registered in the normal module during load. However, the
command is not unregistered at the module unload. So, this may lead to
use-after-free
issue when the normal command is invoked after the normal module unload.

Reported-by: Alec Brown

****

CVE-2025-61664: Missing unregister call for normal_exit command may lead to
use-after-free
CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L - 4.9

The normal_exit command is registered in the normal module during load. However,
the command is not unregistered at the module unload. So, this may lead to

```
use-after-free
issue when the normal_exit command is invoked after the normal module unload.

Reported-by: Alec Brown

******************************************************************************

*** Security recommendation ***

We have observed the same missing unregister behavior for the functional_test
and all_functional_test commands. However, both commands are part of the GRUB's
test library and should not be included in GRUB images targeting production
environments. Given the statement above we opted to not assign CVEs for such
cases and instead strongly recommend that GRUB's users to not include both
functionl_test and all_functional_test commands in the production GRUB images.

******************************************************************************

 grub-core/commands/test.c             |  2 +-
 grub-core/commands/usbtest.c          |  4 ++--
 grub-core/gettext/gettext.c           | 19 ++++++++++++-------
 grub-core/kern/file.c                 |  6 +++---
 grub-core/net/net.c                   |  1 +
 grub-core/normal/main.c               | 12 +++++++-----
 grub-core/tests/lib/functional_test.c |  7 ++++---
 7 files changed, 30 insertions(+), 21 deletions(-)

Alec Brown (3):
      gettext/gettext: Unregister gettext command on module unload
      normal/main: Unregister commands on module unload
      tests/lib/functional_test: Unregister commands on module unload

Jamie (2):
      commands/usbtest: Use correct string length field
      commands/usbtest: Ensure string length is sufficient in usb string
processing

Thomas Frauendorfer | Miray Software (3):
      commands/test: Fix error in recursion depth calculation
      kern/file: Call grub_dl_unref() after fs->fs_close()
      net/net: Unregister net_set_vlan command on unload
```

---

reply via email to
Daniel Kiper

[Prev in Thread] **Current Thread** [Next in Thread]

- **[SECURITY PATCH 0/8] GRUB2 vulnerabilities - 2025/11/18**, *Daniel Kiper* <=
  - **Re: [SECURITY PATCH 0/8] GRUB2 vulnerabilities - 2025/11/18**, *Sudhakar Kuppusamy*, 2025/11/19

- Prev by Date: **[SECURITY PATCH 1/8] commands/test: Fix error in recursion depth calculation**
- Next by Date: **[SECURITY PATCH 1/8] commands/test: Fix error in recursion depth calculation**
- Previous by thread: **[SECURITY PATCH 1/8] commands/test: Fix error in recursion depth calculation**
- Next by thread: **Re: [SECURITY PATCH 0/8] GRUB2 vulnerabilities - 2025/11/18**
- Index(es):

- **Date**
- **Thread**