

Foreman - Feature #37345

Improve "EFI local chainloading" on SecureBoot enabled hosts

04/11/2024 11:36 AM - Jan Loeser

<div>Status: Ready For Testing</div> <div>Priority: Normal</div> <div>Assignee:</div> <div>Category:</div> <div>Target version:</div> <div>Difficulty:</div> <div>Triaged: No</div> <div>Bugzilla link:</div> <div>Pull request: https://github.com/theforeman/foreman/pull/10126</div>	<div>Fixed in Releases:</div> <div>Found in Releases:</div> <div>Red Hat JIRA:</div>
<div>Description</div> <p>Chainloading is not supported when SecureBoot is enabled [1].</p> <p>Currently, this issue is tried to be tackled by changing the boot order during installation to boot from disk by default. But this disturbs the "always boot from network" workflow which might result in broken attempts for the user to re-provision a host (see https://github.com/theforeman/foreman/pull/9123).</p> <p>What we can do is to exit network booted GRUB2 with `exit 1` resulting in the boot of the next boot device, which is probably the boot file from disk.</p> <p>The use of efibootmgr_netboot is still possible (if desired).</p> <p>The proposed solution would also work when SecureBoot is disabled, however to avoid side effects I propose to only boot next device if SecureBoot is enabled (GRUB2 variable `lockdown=y` [2]).</p> <p>[1]: https://www.gnu.org/software/grub/manual/grub/grub.html#UEFI-secure-boot-and-shim</p> <p>[2]: https://www.gnu.org/software/grub/manual/grub/grub.html#Lockdown</p>	

History

- #1 - 04/11/2024 11:41 AM - The Foreman Bot
- Status changed from New to Ready For Testing
 - Pull request <https://github.com/theforeman/foreman/pull/10126> added