<Chat> Linux-Surface Kernel Developer

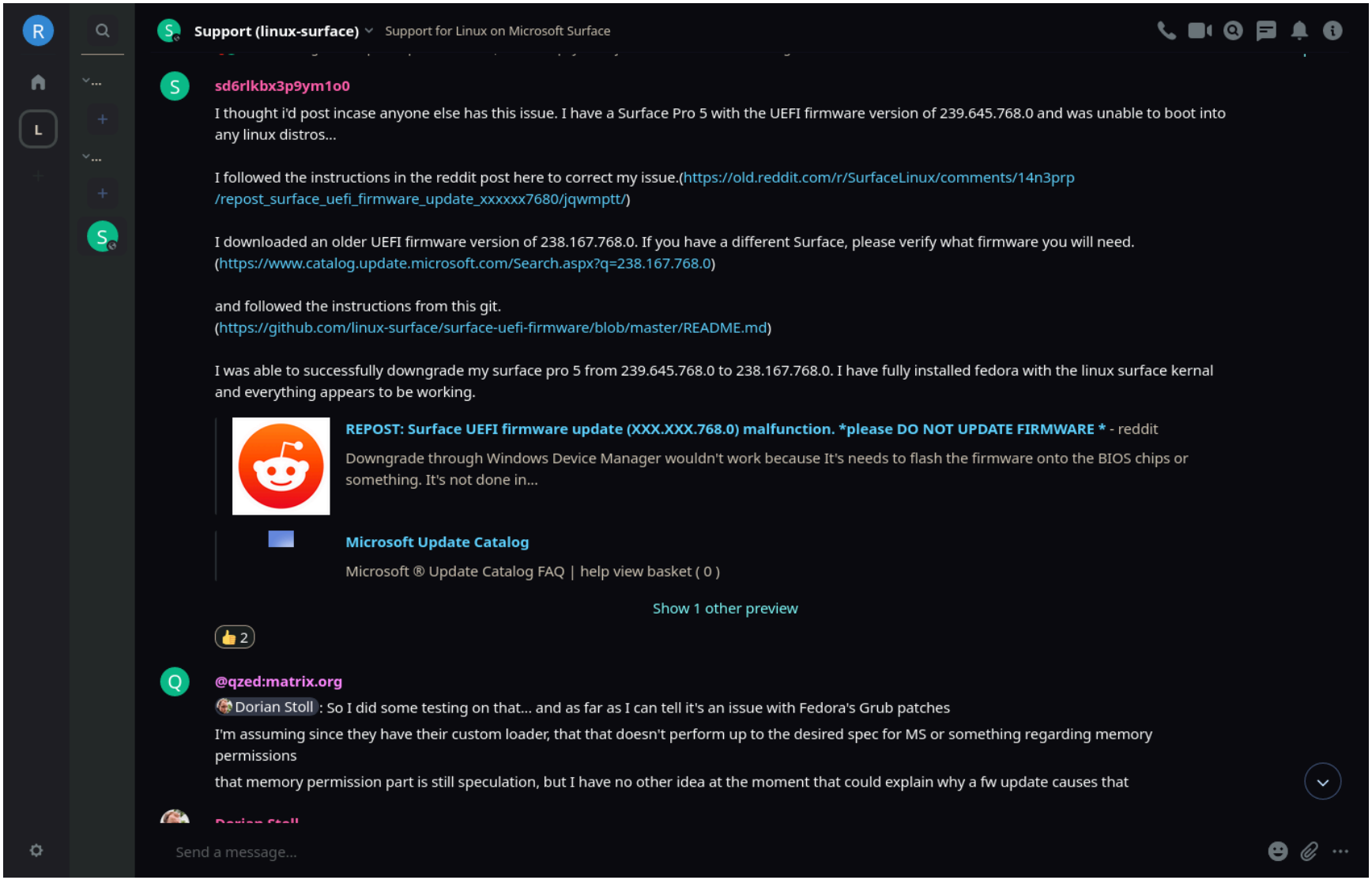
This is another document including groups of screenshots captured from Support (linux-surface) , It's the discussion of the root cause.

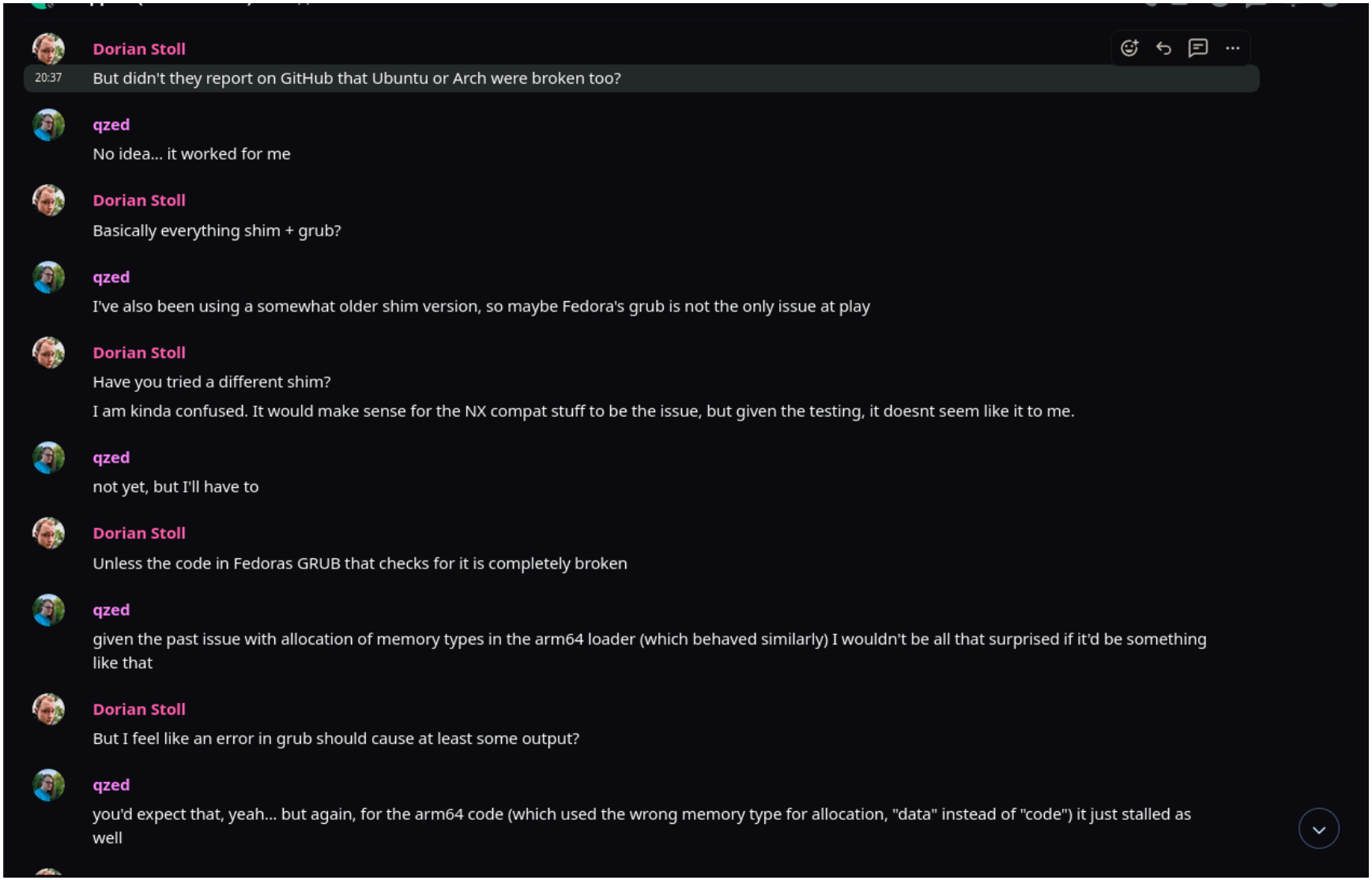
Some screenshots might not be useful/ not related to the issue but I still put them here anyway, in case anyone loses track of the date of the chat or the trend of what It's talking about.

I've marked groups of chats that I think are useful to understand the issue, with <USEFUL>

[Sat, Jul 8 2023]

New Surface UEFI firmware enforces this NX security option?


Support (linux-surface)
Support for Linux on Microsoft Surface
sd6rlkbx3p9ym1o0
I thought i'd post incase anyone else has this issue. I have a Surface Pro 5 with the UEFI firmware version of 239.645.768.0 and was unable to boot into any linux distros...
I followed the instructions in the reddit post here to correct my issue.(https://old.reddit.com/r/SurfaceLinux/comments/14n3prp/repost_surface_uefi_firmware_update_xxxxxx7680/jqwmptt/)
I downloaded an older UEFI firmware version of 238.167.768.0. If you have a different Surface, please verify what firmware you will need. (https://www.catalog.update.microsoft.com/Search.aspx?q=238.167.768.0)
and followed the instructions from this git. (https://github.com/linux-surface/surface-uefi-firmware/blob/master/README.md)
I was able to successfully downgrade my surface pro 5 from 239.645.768.0 to 238.167.768.0. I have fully installed fedora with the linux surface kernal and everything appears to be working.
REPOST: Surface UEFI firmware update (XXX.XXX.768.0) malfunction. *please DO NOT UPDATE FIRMWARE * - reddit
Downgrade through Windows Device Manager wouldn't work because It's needs to flash the firmware onto the BIOS chips or something. It's not done in...
Microsoft Update Catalog
Microsoft ® Update Catalog FAQ | help view basket (0)
Show 1 other preview
2
@qzed:matrix.org
Dorian Stoll : So I did some testing on that... and as far as I can tell it's an issue with Fedora's Grub patches
I'm assuming since they have their custom loader, that that doesn't perform up to the desired spec for MS or something regarding memory permissions
that memory permission part is still speculation, but I have no other idea at the moment that could explain why a fw update causes that
Send a message...



Dorian Stoll

20:37 But didn't they report on GitHub that Ubuntu or Arch were broken too?

qzed

No idea... it worked for me

Dorian Stoll

Basically everything shim + grub?

qzed

I've also been using a somewhat older shim version, so maybe Fedora's grub is not the only issue at play

Dorian Stoll

Have you tried a different shim?

I am kinda confused. It would make sense for the NX compat stuff to be the issue, but given the testing, it doesnt seem like it to me.

qzed

not yet, but I'll have to

Dorian Stoll

Unless the code in Fedoras GRUB that checks for it is completely broken

qzed

given the past issue with allocation of memory types in the arm64 loader (which behaved similarly) I wouldn't be all that surprised if it'd be something like that

Dorian Stoll

But I feel like an error in grub should cause at least some output?

qzed

you'd expect that, yeah... but again, for the arm64 code (which used the wrong memory type for allocation, "data" instead of "code") it just stalled as well

<USEFUL>

Some firmware protection thing kicks in and essentially stalls things without grub even having a chance to figure out something is going wrong

Dorian Stoll

21:14 GRUB ...

if we need a turing complete bootloader why cant we just use linuxboot? xD

😆 1

qzed

if I understand correctly, some firmware protection thing kicks in and essentially stalls things without grub even having a chance to figure out something is going wrong

I'll try the latest shim version this evening, then we can see if there's another issue

Dorian Stoll

https://github.com/rhboot/grub2/blob/fedora-39/grub-core/loader/efi/chainloader.c#L597

grub2/grub-core/loader/efi/chainloader.c at fedora-39 · rhboot/grub2 - GitHub

Ongoing downstream work on grub2, including Fedora and RHEL. ***This is not upstream; please send code upstream first*** - rhboot/grub2

that also says data

and the error from calling the entrypoint of the binary is just ignored. so grub shuts down because it thinks its done

Dorian Stoll

but that part of the code only runs when secureboot is enabled?

this makes no sense

qzed

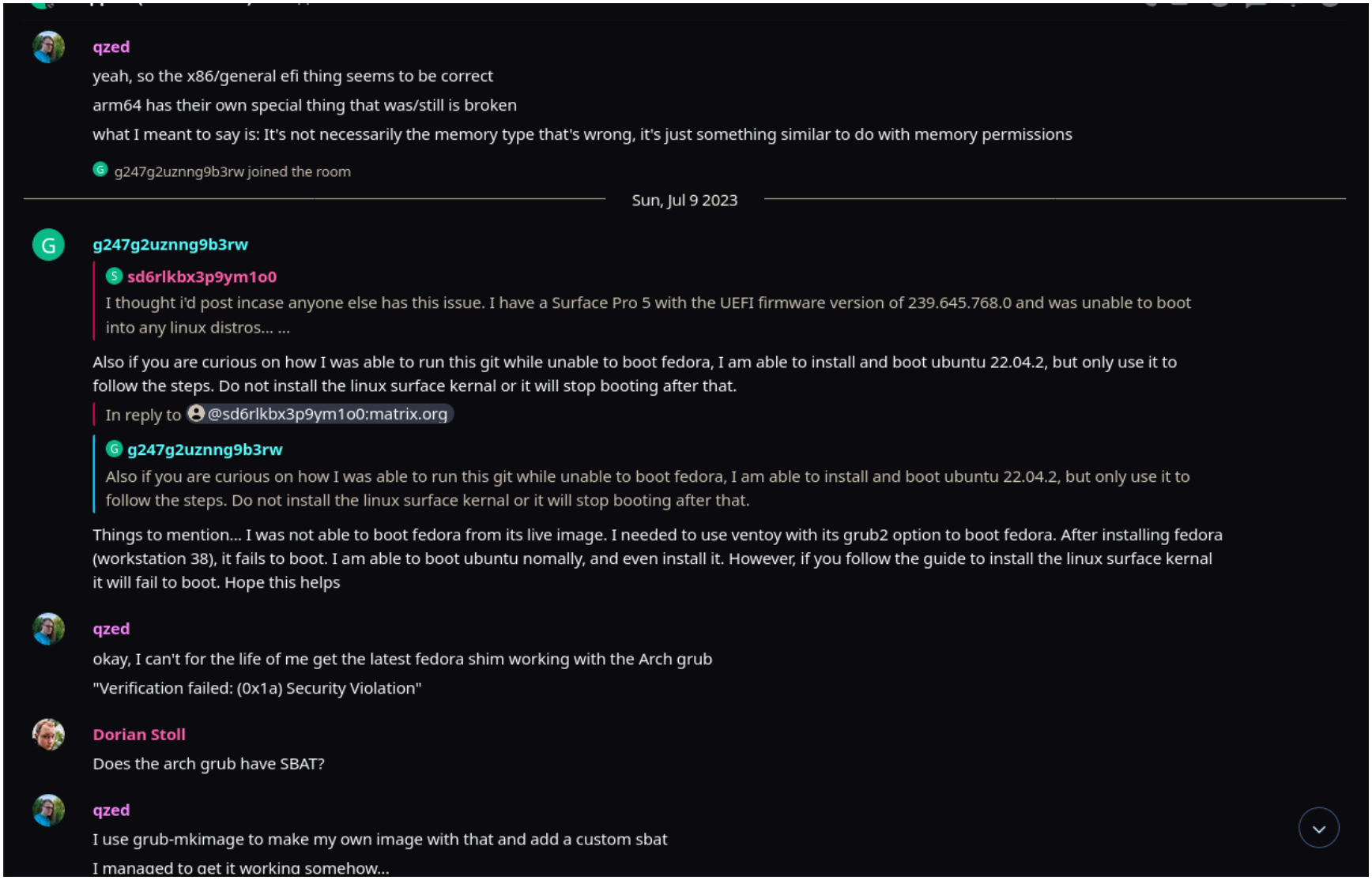
Shouldn't that be an issue in linux.c fand not chainloader?

Dorian Stoll

right

but that uses GRUB_EFI_LOADER_CODE

qzed



qzed

yeah, so the x86/general efi thing seems to be correct

arm64 has their own special thing that was/still is broken

what I meant to say is: It's not necessarily the memory type that's wrong, it's just something similar to do with memory permissions

g247g2uznng9b3rw joined the room

Sun, Jul 9 2023

g247g2uznng9b3rw

> **sd6rlkbx3p9ym1o0**
> I thought i'd post incase anyone else has this issue. I have a Surface Pro 5 with the UEFI firmware version of 239.645.768.0 and was unable to boot into any linux distros... ...

Also if you are curious on how I was able to run this git while unable to boot fedora, I am able to install and boot ubuntu 22.04.2, but only use it to follow the steps. Do not install the linux surface kernal or it will stop booting after that.

> In reply to @sd6rlkbx3p9ym1o0:matrix.org
>
> > **g247g2uznng9b3rw**
> > Also if you are curious on how I was able to run this git while unable to boot fedora, I am able to install and boot ubuntu 22.04.2, but only use it to follow the steps. Do not install the linux surface kernal or it will stop booting after that.

Things to mention... I was not able to boot fedora from its live image. I needed to use ventoy with its grub2 option to boot fedora. After installing fedora (workstation 38), it fails to boot. I am able to boot ubuntu nomally, and even install it. However, if you follow the guide to install the linux surface kernal it will fail to boot. Hope this helps

qzed

okay, I can't for the life of me get the latest fedora shim working with the Arch grub

"Verification failed: (0x1a) Security Violation"

Dorian Stoll

Does the arch grub have SBAT?

qzed

I use grub-mkimage to make my own image with that and add a custom sbat

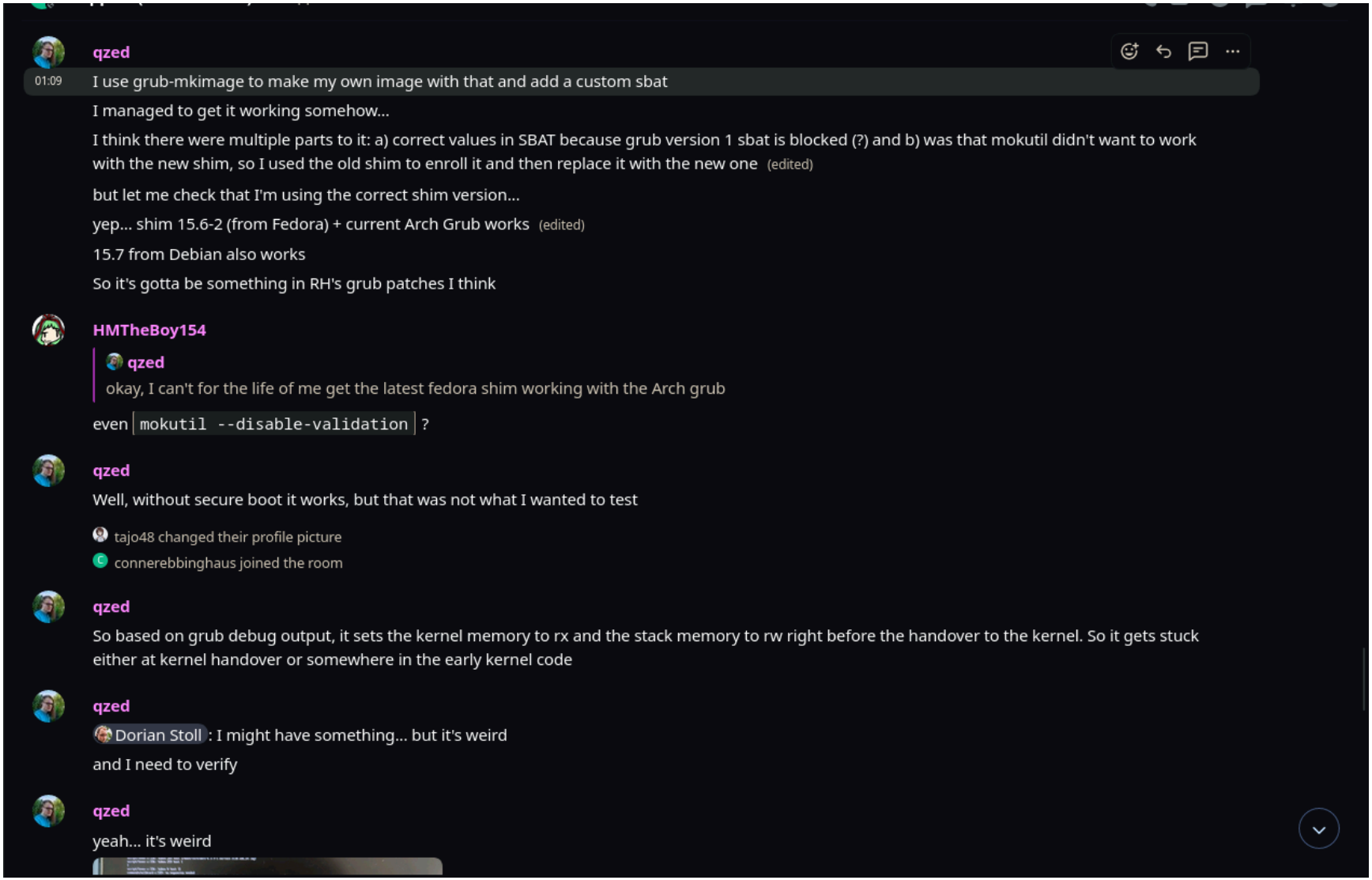
I managed to get it working somehow...

<USEFUL>

Why does the kernel memory need write permissions?

So based on grub debug output, it sets the kernel memory to `rx` and the stack memory to `rw` right before the handover to the kernel.

So it gets stuck either at kernel handover or somewhere in the early kernel code


qzed
01:09
I use grub-mkimage to make my own image with that and add a custom sbat
I managed to get it working somehow...
I think there were multiple parts to it: a) correct values in SBAT because grub version 1 sbat is blocked (?) and b) was that mokutil didn't want to work with the new shim, so I used the old shim to enroll it and then replace it with the new one (edited)
but let me check that I'm using the correct shim version...
yep... shim 15.6-2 (from Fedora) + current Arch Grub works (edited)
15.7 from Debian also works
So it's gotta be something in RH's grub patches I think
HMTheBoy154
qzed
okay, I can't for the life of me get the latest fedora shim working with the Arch grub
even mokutil --disable-validation ?
qzed
Well, without secure boot it works, but that was not what I wanted to test
tajo48 changed their profile picture
connerebbinghaus joined the room
qzed
So based on grub debug output, it sets the kernel memory to rx and the stack memory to rw right before the handover to the kernel. So it gets stuck either at kernel handover or somewhere in the early kernel code
qzed
Dorian Stoll : I might have something... but it's weird
and I need to verify
qzed
yeah... it's weird

0:00 / 0:00

22:00 notice the last couple of lines

in particular: `permissions for <kernel memory> are rwx` and `permissions for <stack> are rwx`

before, they were `r-x` and `rw-`

so... it doesn't boot if we follow the nx stuff and it boots if we just mark everything as `rwx` ?!

qzed

```
diff --git a/grub-core/loader/efi/linux.c b/grub-core/loader/efi/linux.c
index e413bdcc2..532b26432 100644
--- a/grub-core/loader/efi/linux.c
+++ b/grub-core/loader/efi/linux.c
@@ -173,8 +173,8 @@ grub_efi_linux_boot (grub_addr_t kernel_addr, grub_size_t kernel_size,

   if (nx_supported)
     {
-      kernel_set_attrs &= ~GRUB_MEM_ATTR_W;
-      kernel_clear_attrs |= GRUB_MEM_ATTR_W;
+      // kernel_set_attrs &= ~GRUB_MEM_ATTR_W;
+      // kernel_clear_attrs |= GRUB_MEM_ATTR_W;
       stack_set_attrs &= ~GRUB_MEM_ATTR_X;
       stack_clear_attrs |= GRUB_MEM_ATTR_X;
     }
```

the minimal change that makes this work

essentially, that changes kernel memory to `rwx`

(instead of `r-x`)

qzed

at least all of that works without secureboot, haven't checked with secureboot yet

qzed

and with secureboot it works as well

notice the last couple of lines
in particular: permissions for <kernel memory> are rwx and permissions for <stack> are rwx
before, they were r-x and rw-
so... it doesn't boot if we follow the nx stuff and it boots if we just mark everything as rwx?!

```
diff --git a/grub-core/loader/efi/linux.c b/grub-core/loader/efi/linux.c
index e413bdcc2..532b26432 100644
--- a/grub-core/loader/efi/linux.c
+++ b/grub-core/loader/efi/linux.c
@@ -173,8 +173,8 @@ grub_efi_linux_boot (grub_addr_t kernel_addr, grub_size_t kernel_size,

   if (nx_supported)
     {
-      kernel_set_attrs &= ~GRUB_MEM_ATTR_W;
-      kernel_clear_attrs |= GRUB_MEM_ATTR_W;
+      // kernel_set_attrs &= ~GRUB_MEM_ATTR_W;
+      // kernel_clear_attrs |= GRUB_MEM_ATTR_W;
       stack_set_attrs &= ~GRUB_MEM_ATTR_X;
       stack_clear_attrs |= GRUB_MEM_ATTR_X;
     }
```

the minimal change that makes this work. essentially, that changes kernel memory to rwx
(instead of r-x)

at least all of that works without secureboot, haven't checked with secureboot yet
and with secureboot it works as well

could it be related to the decompression done by the stub before jumping to the actual kernel?
I believe that the EFI stub adjusts the memory permissions and removes the write protection from the image here:
https://github.com/torvalds/linux/blob/master/drivers/firmware/efi/libstub/x86-stub.c#L296-L322
and I think the grub loader skips the EFI stub, so the memory is protected by default from the firmware and the protection is never removed?

[Mon, Jul 17 2023]

Fedora GRUB problem or Surface UEFI Problem?

Support (linux-surface) Support for Linux on Microsoft Surface

Mon, Jul 17 2023

Ramen-LadyHKG

UEFI firmware malfunction

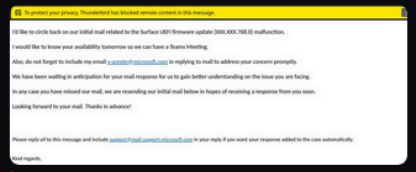
[Update "6" - Surface Business Support meeting] 17th-July, 2023

1. The issue is discovered --- ✅
2. The issue is confirmed exist on other users --- ✅
3. The issue is reported to Microsoft --- ✅
4. **Temporary solution is found ---** ✅
5. The issue is confirmed by Microsoft --- 🟩
6. The issue is fixed by Microsoft --- 🟩

Here's some update, I received Microsoft reply to my support ticket.
We're going to have a MS Meet and discuss this problem, I will talk about `Surface Pro` series as well not just `Book`

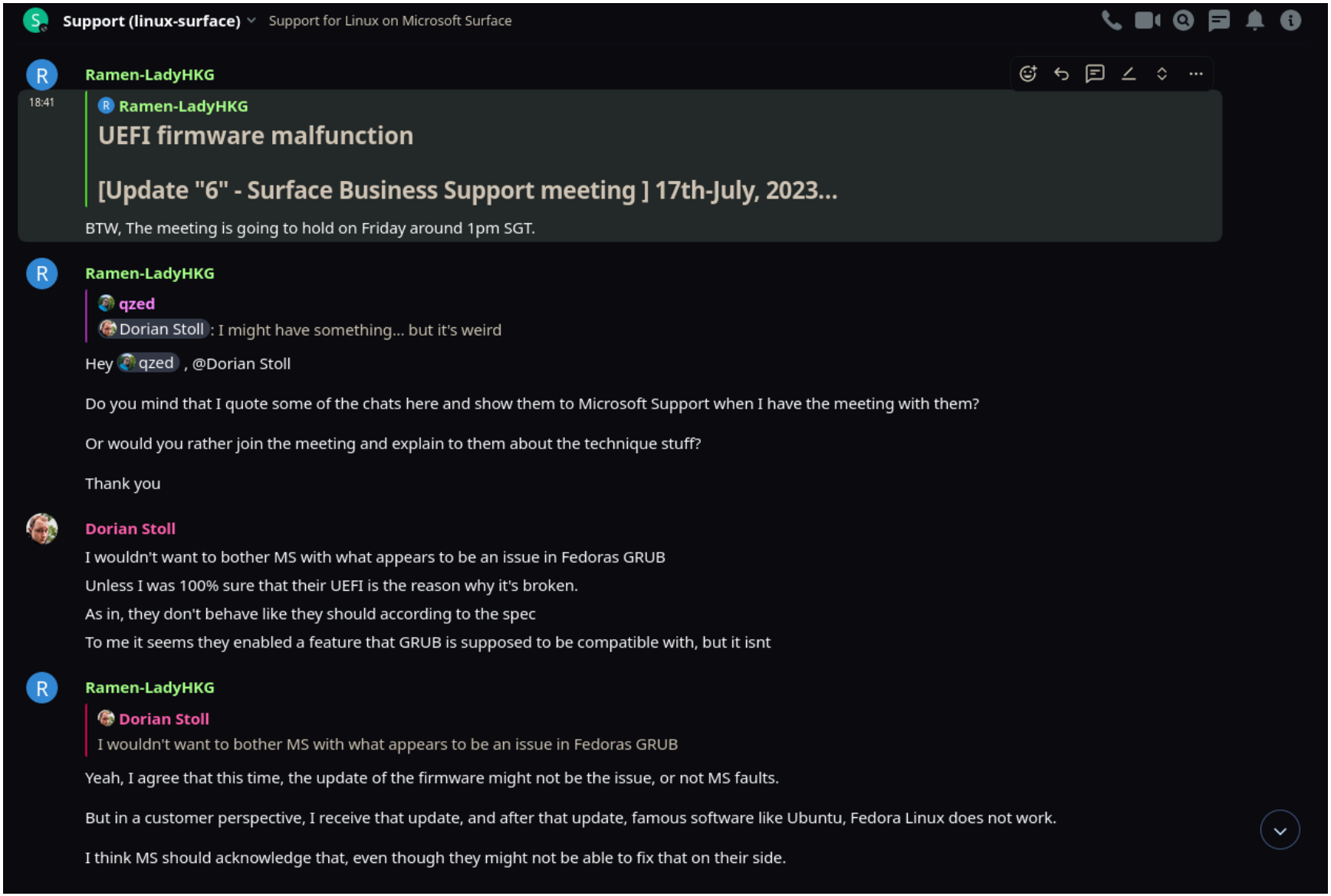
If you have anything related need to tell them or you want to join the meeting.
Or any information that helps us resolve this issue.
Please do let me know
(edited)

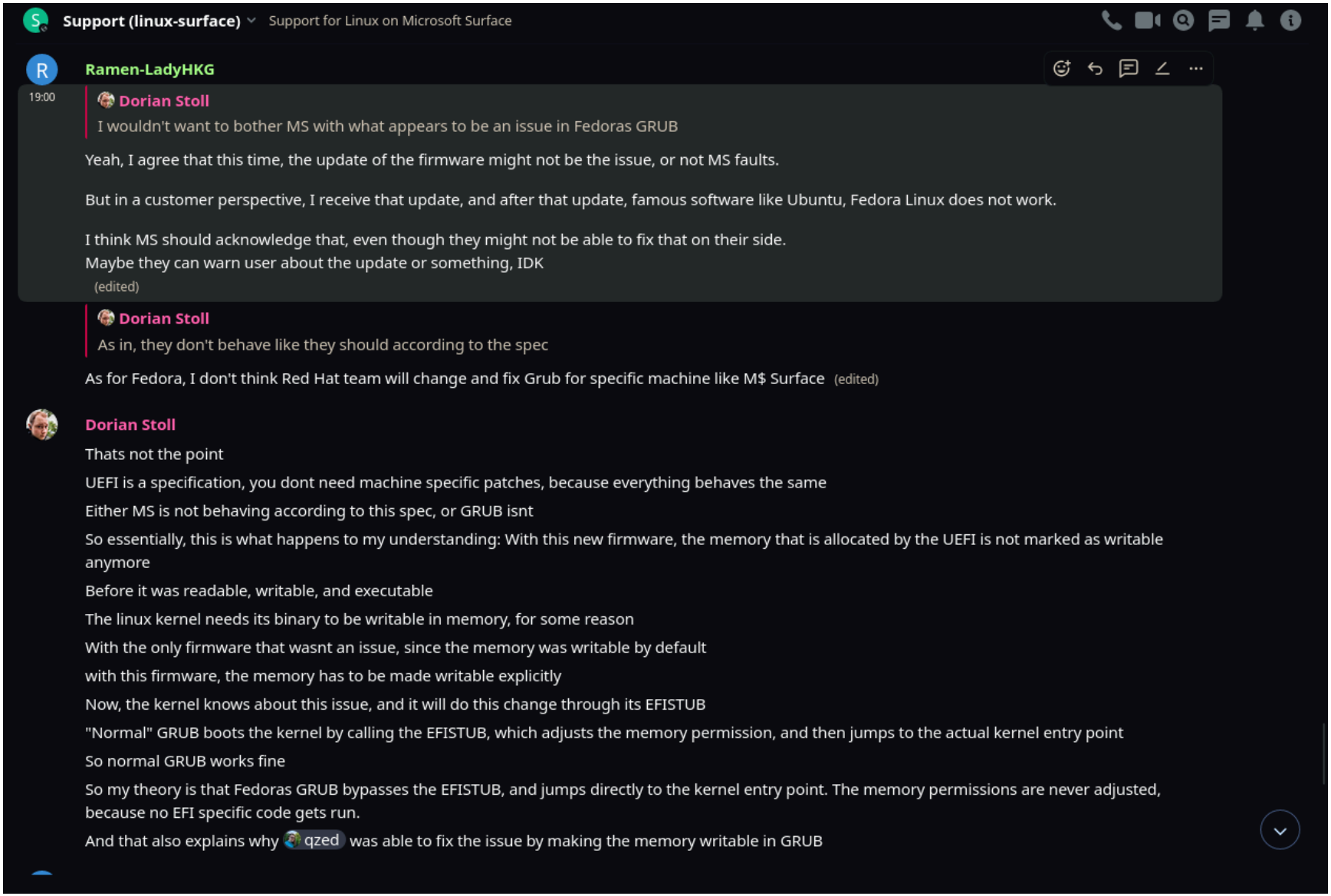
> **sd6rlkbx3p9ym1o0**
> I thought i'd post incase anyone else has this issue. I have a Surface Pro 5 with the UEFI firmware version of 239.645.768.0 and was unable to boot into any linux distros... ...

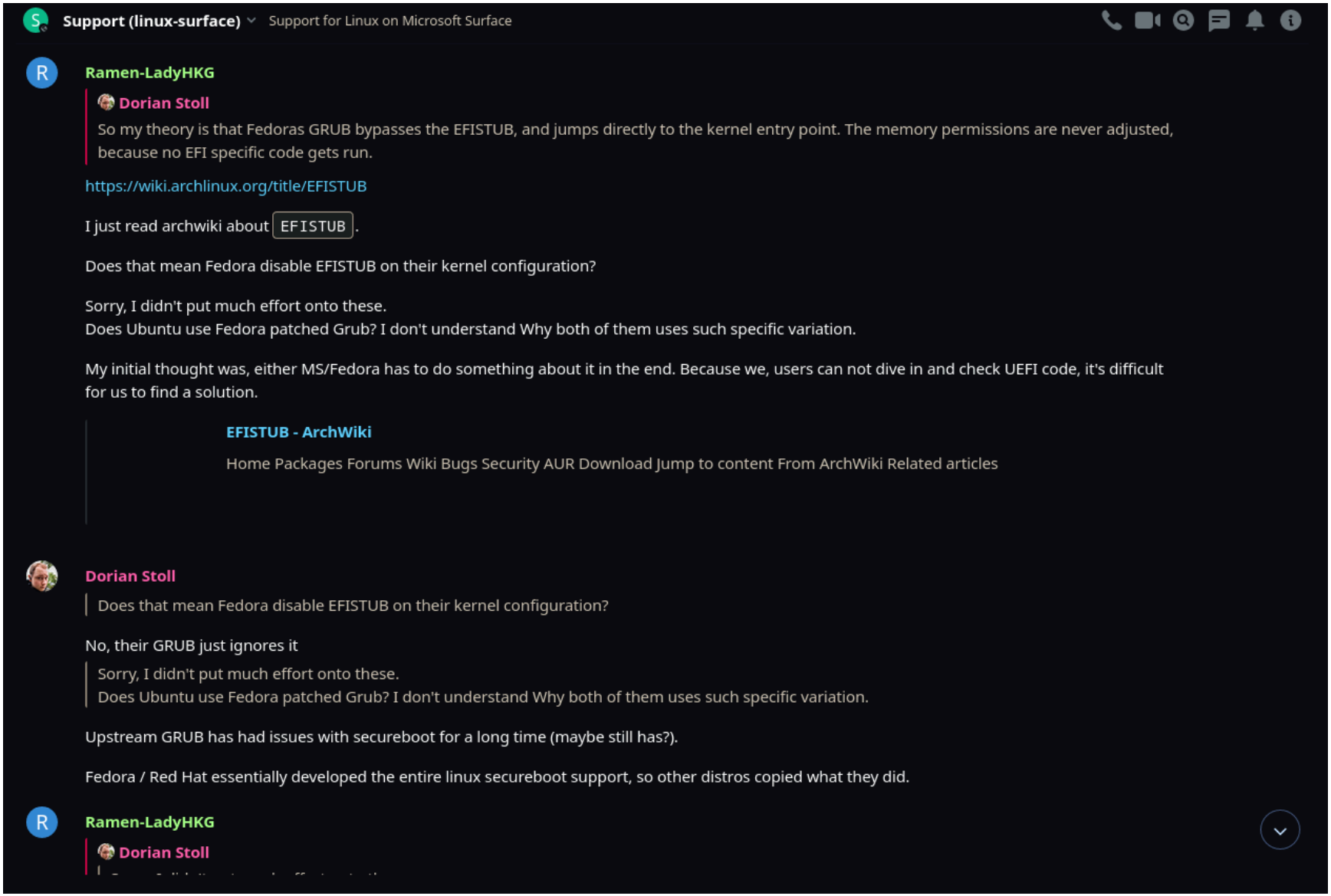


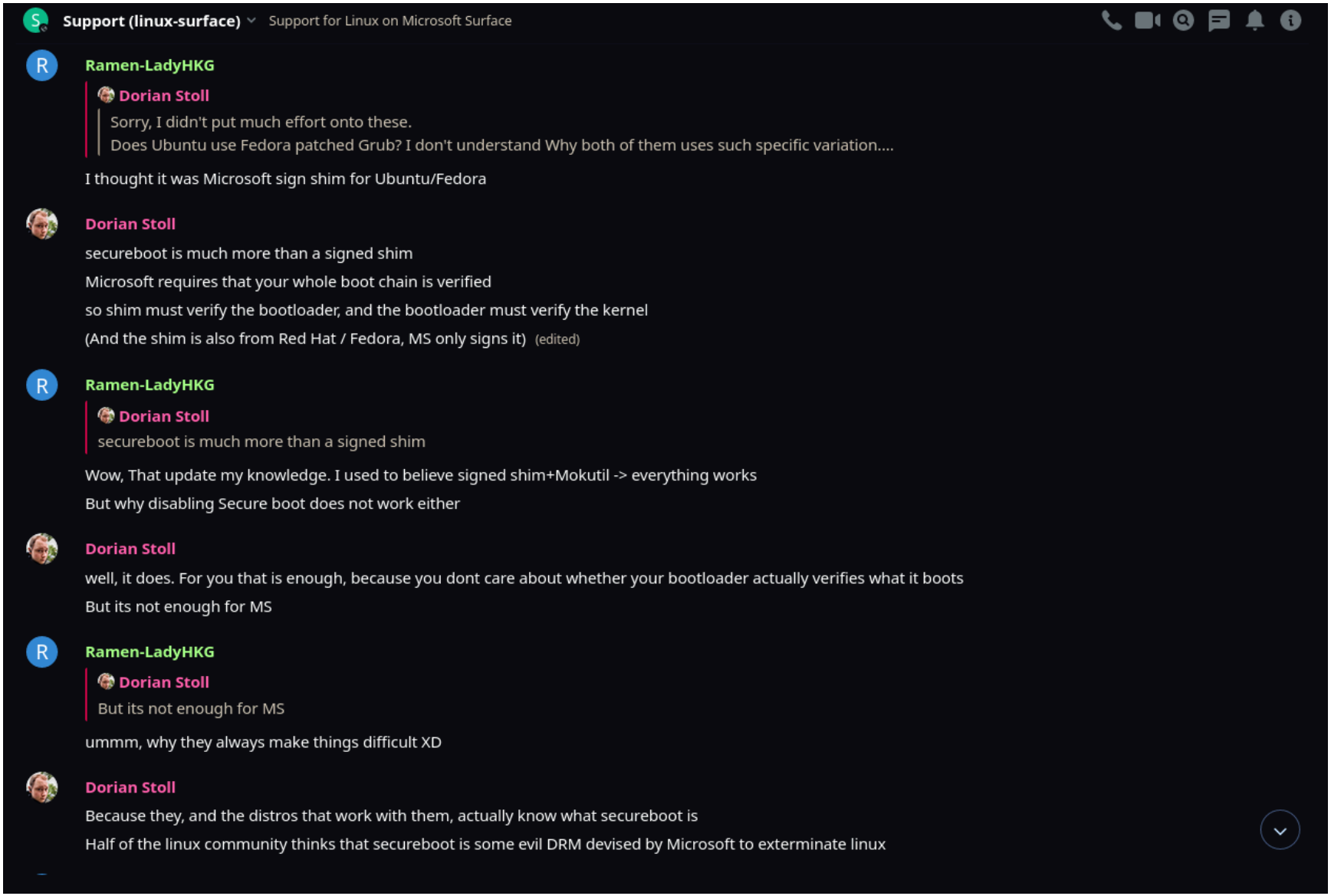
> **sd6rlkbx3p9ym1o0**
> I thought i'd post incase anyone else has this issue. I have a Surface Pro 5 with the UEFI firmware version of 239.645.768.0 and was unable to boot into any linux distros... ...

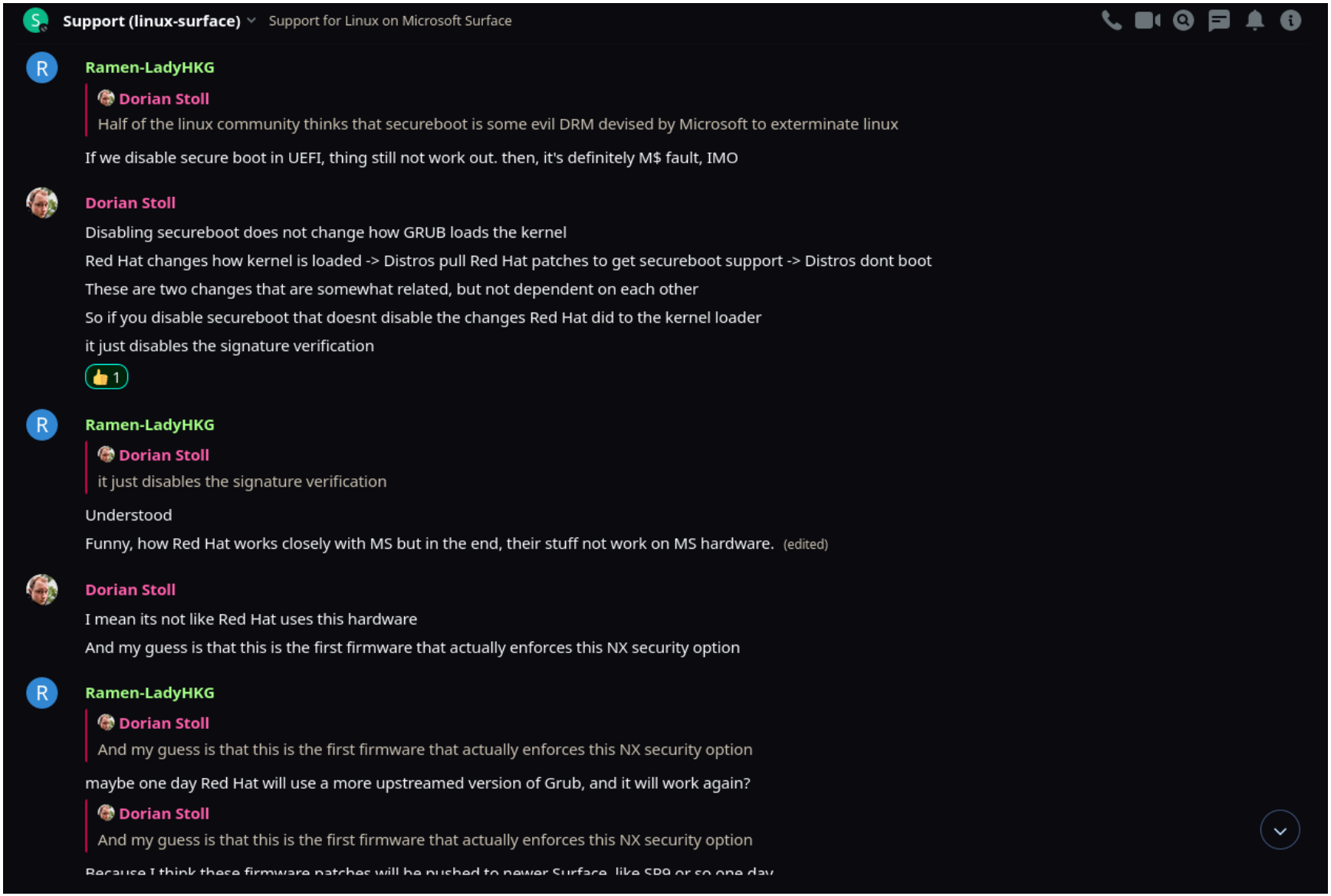
Send a message...

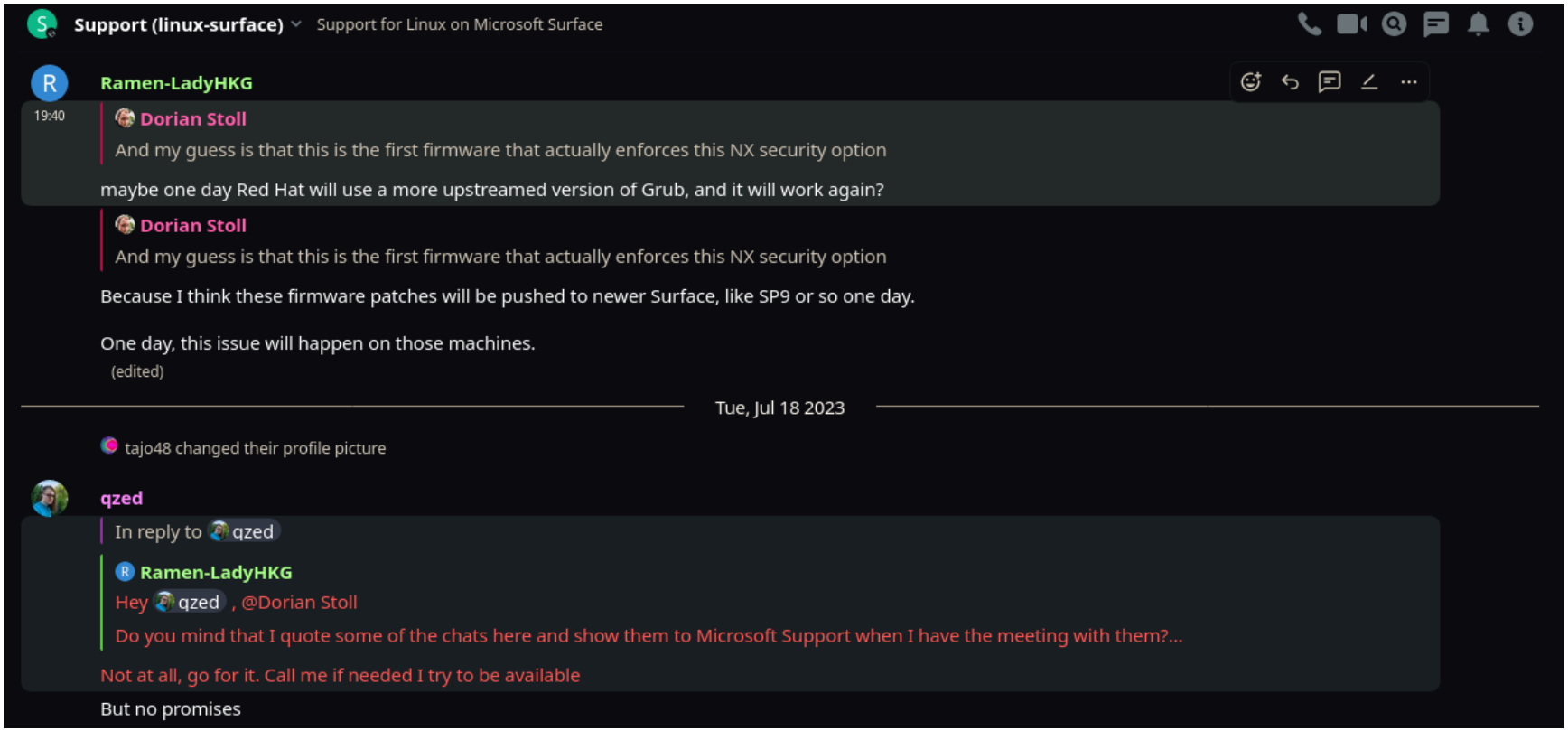

Support (linux-surface)
Support for Linux on Microsoft Surface
Ramen-LadyHKG
18:41
Ramen-LadyHKG
UEFI firmware malfunction
[Update "6" - Surface Business Support meeting] 17th-July, 2023...
BTW, The meeting is going to hold on Friday around 1pm SGT.
Ramen-LadyHKG
qzed
Dorian Stoll: I might have something... but it's weird
Hey qzed , @Dorian Stoll
Do you mind that I quote some of the chats here and show them to Microsoft Support when I have the meeting with them?
Or would you rather join the meeting and explain to them about the technique stuff?
Thank you
Dorian Stoll
I wouldn't want to bother MS with what appears to be an issue in Fedoras GRUB
Unless I was 100% sure that their UEFI is the reason why it's broken.
As in, they don't behave like they should according to the spec
To me it seems they enabled a feature that GRUB is supposed to be compatible with, but it isnt
Ramen-LadyHKG
Dorian Stoll
I wouldn't want to bother MS with what appears to be an issue in Fedoras GRUB
Yeah, I agree that this time, the update of the firmware might not be the issue, or not MS faults.
But in a customer perspective, I receive that update, and after that update, famous software like Ubuntu, Fedora Linux does not work.
I think MS should acknowledge that, even though they might not be able to fix that on their side.


Support (linux-surface)
Support for Linux on Microsoft Surface
Ramen-LadyHKG
19:00
Dorian Stoll
I wouldn't want to bother MS with what appears to be an issue in Fedoras GRUB
Yeah, I agree that this time, the update of the firmware might not be the issue, or not MS faults.
But in a customer perspective, I receive that update, and after that update, famous software like Ubuntu, Fedora Linux does not work.
I think MS should acknowledge that, even though they might not be able to fix that on their side.
Maybe they can warn user about the update or something, IDK
(edited)
Dorian Stoll
As in, they don't behave like they should according to the spec
As for Fedora, I don't think Red Hat team will change and fix Grub for specific machine like M$ Surface (edited)
Dorian Stoll
Thats not the point
UEFI is a specification, you dont need machine specific patches, because everything behaves the same
Either MS is not behaving according to this spec, or GRUB isnt
So essentially, this is what happens to my understanding: With this new firmware, the memory that is allocated by the UEFI is not marked as writable anymore
Before it was readable, writable, and executable
The linux kernel needs its binary to be writable in memory, for some reason
With the only firmware that wasnt an issue, since the memory was writable by default
with this firmware, the memory has to be made writable explicitly
Now, the kernel knows about this issue, and it will do this change through its EFISTUB
"Normal" GRUB boots the kernel by calling the EFISTUB, which adjusts the memory permission, and then jumps to the actual kernel entry point
So normal GRUB works fine
So my theory is that Fedoras GRUB bypasses the EFISTUB, and jumps directly to the kernel entry point. The memory permissions are never adjusted, because no EFI specific code gets run.
And that also explains why qzed was able to fix the issue by making the memory writable in GRUB

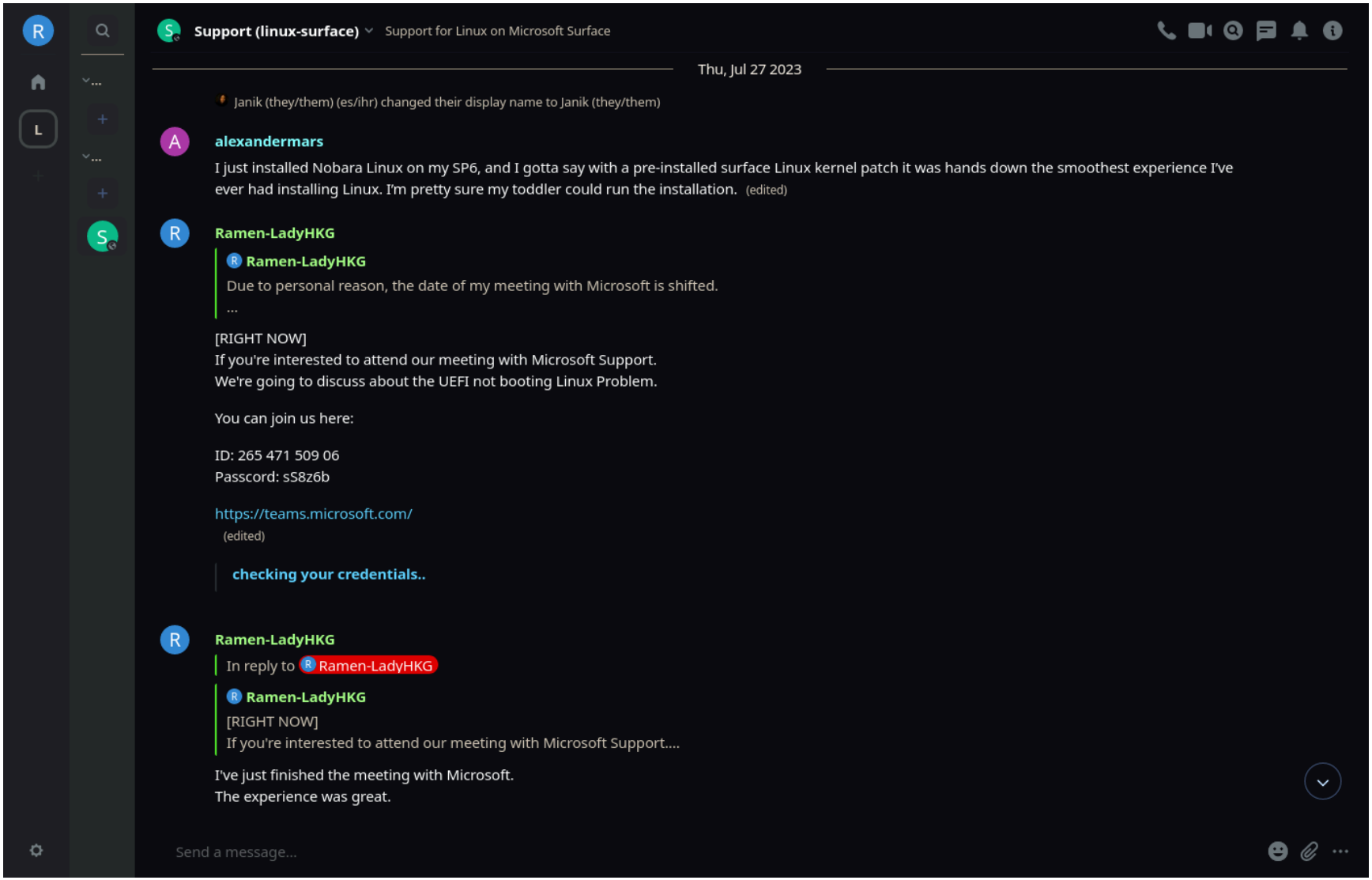

Support (linux-surface)
Support for Linux on Microsoft Surface
Ramen-LadyHKG
Dorian Stoll
So my theory is that Fedoras GRUB bypasses the EFISTUB, and jumps directly to the kernel entry point. The memory permissions are never adjusted, because no EFI specific code gets run.
https://wiki.archlinux.org/title/EFISTUB
I just read archwiki about EFISTUB.
Does that mean Fedora disable EFISTUB on their kernel configuration?
Sorry, I didn't put much effort onto these.
Does Ubuntu use Fedora patched Grub? I don't understand Why both of them uses such specific variation.
My initial thought was, either MS/Fedora has to do something about it in the end. Because we, users can not dive in and check UEFI code, it's difficult for us to find a solution.
EFISTUB - ArchWiki
Home Packages Forums Wiki Bugs Security AUR Download Jump to content From ArchWiki Related articles
Dorian Stoll
Does that mean Fedora disable EFISTUB on their kernel configuration?
No, their GRUB just ignores it
Sorry, I didn't put much effort onto these.
Does Ubuntu use Fedora patched Grub? I don't understand Why both of them uses such specific variation.
Upstream GRUB has had issues with secureboot for a long time (maybe still has?).
Fedora / Red Hat essentially developed the entire linux secureboot support, so other distros copied what they did.
Ramen-LadyHKG
Dorian Stoll

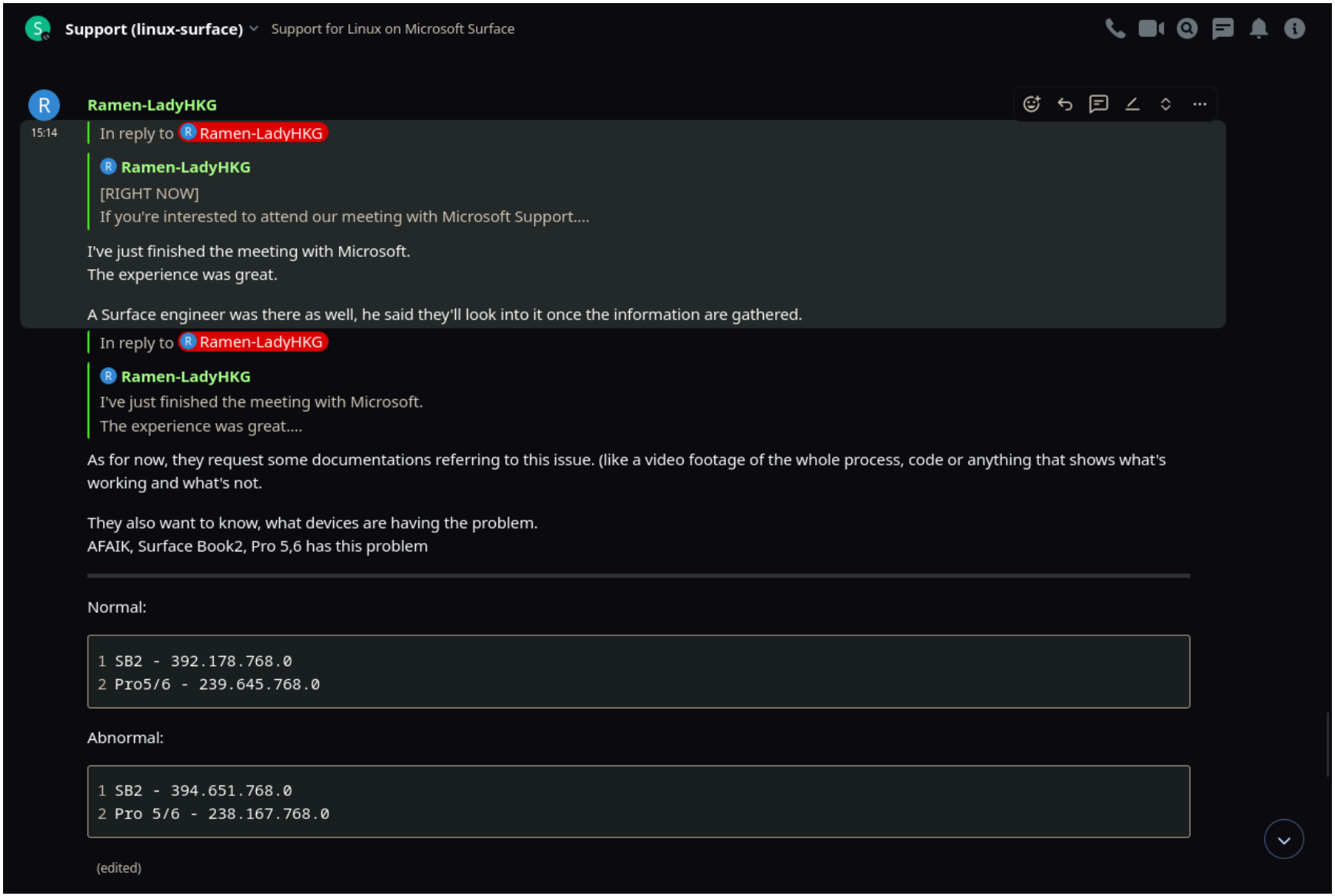

Support (linux-surface)
Support for Linux on Microsoft Surface
Ramen-LadyHKG
Dorian Stoll
Sorry, I didn't put much effort onto these.
Does Ubuntu use Fedora patched Grub? I don't understand Why both of them uses such specific variation....
I thought it was Microsoft sign shim for Ubuntu/Fedora
Dorian Stoll
secureboot is much more than a signed shim
Microsoft requires that your whole boot chain is verified
so shim must verify the bootloader, and the bootloader must verify the kernel
(And the shim is also from Red Hat / Fedora, MS only signs it) (edited)
Ramen-LadyHKG
Dorian Stoll
secureboot is much more than a signed shim
Wow, That update my knowledge. I used to believe signed shim+Mokutil -> everything works
But why disabling Secure boot does not work either
Dorian Stoll
well, it does. For you that is enough, because you dont care about whether your bootloader actually verifies what it boots
But its not enough for MS
Ramen-LadyHKG
Dorian Stoll
But its not enough for MS
ummm, why they always make things difficult XD
Dorian Stoll
Because they, and the distros that work with them, actually know what secureboot is
Half of the linux community thinks that secureboot is some evil DRM devised by Microsoft to exterminate linux

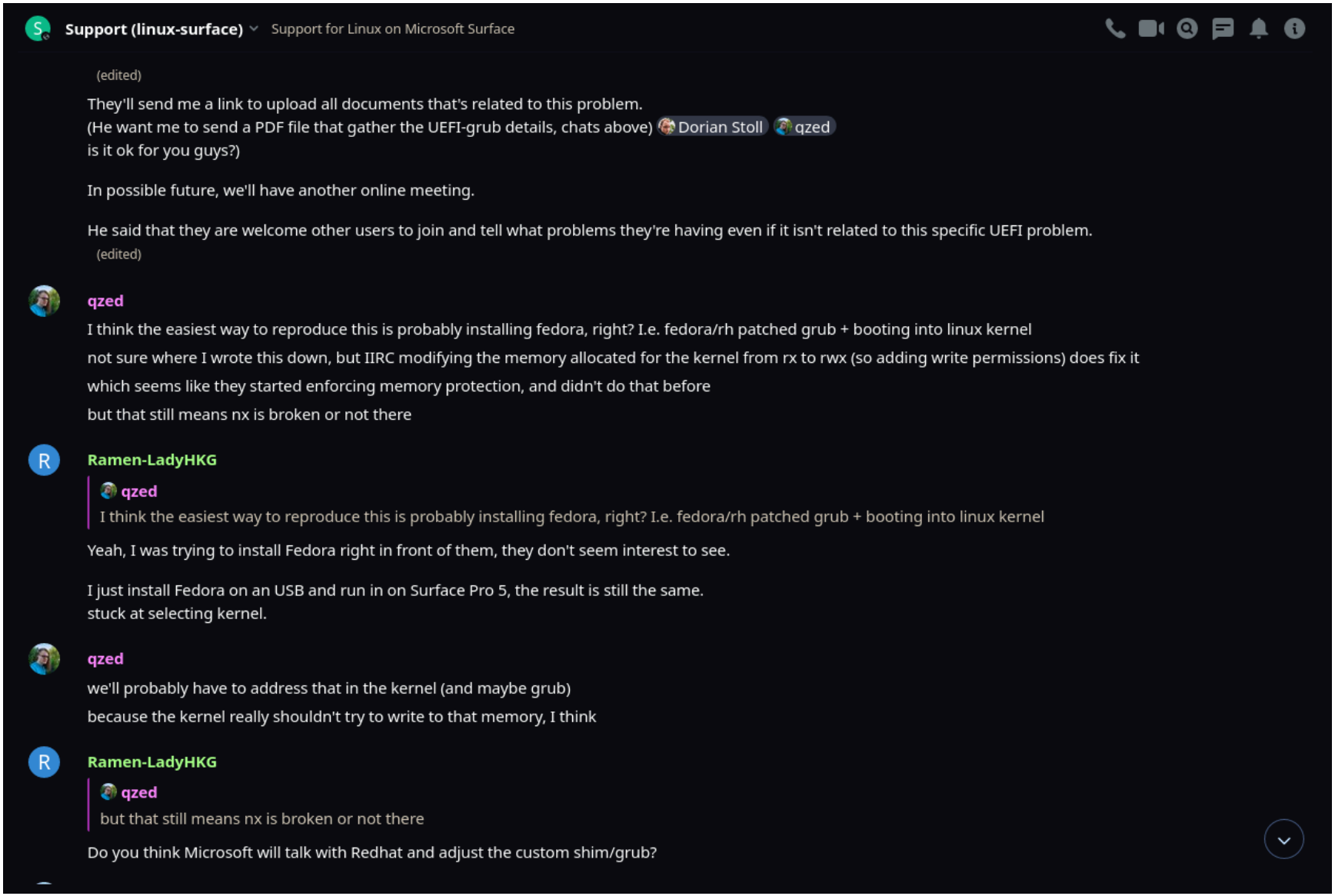

Support (linux-surface)
Support for Linux on Microsoft Surface
Ramen-LadyHKG
Dorian Stoll
Half of the linux community thinks that secureboot is some evil DRM devised by Microsoft to exterminate linux
If we disable secure boot in UEFI, thing still not work out. then, it's definitely M$ fault, IMO
Dorian Stoll
Disabling secureboot does not change how GRUB loads the kernel
Red Hat changes how kernel is loaded -> Distros pull Red Hat patches to get secureboot support -> Distros dont boot
These are two changes that are somewhat related, but not dependent on each other
So if you disable secureboot that doesnt disable the changes Red Hat did to the kernel loader
it just disables the signature verification
1
Ramen-LadyHKG
Dorian Stoll
it just disables the signature verification
Understood
Funny, how Red Hat works closely with MS but in the end, their stuff not work on MS hardware. (edited)
Dorian Stoll
I mean its not like Red Hat uses this hardware
And my guess is that this is the first firmware that actually enforces this NX security option
Ramen-LadyHKG
Dorian Stoll
And my guess is that this is the first firmware that actually enforces this NX security option
maybe one day Red Hat will use a more upstreamed version of Grub, and it will work again?
Dorian Stoll
And my guess is that this is the first firmware that actually enforces this NX security option

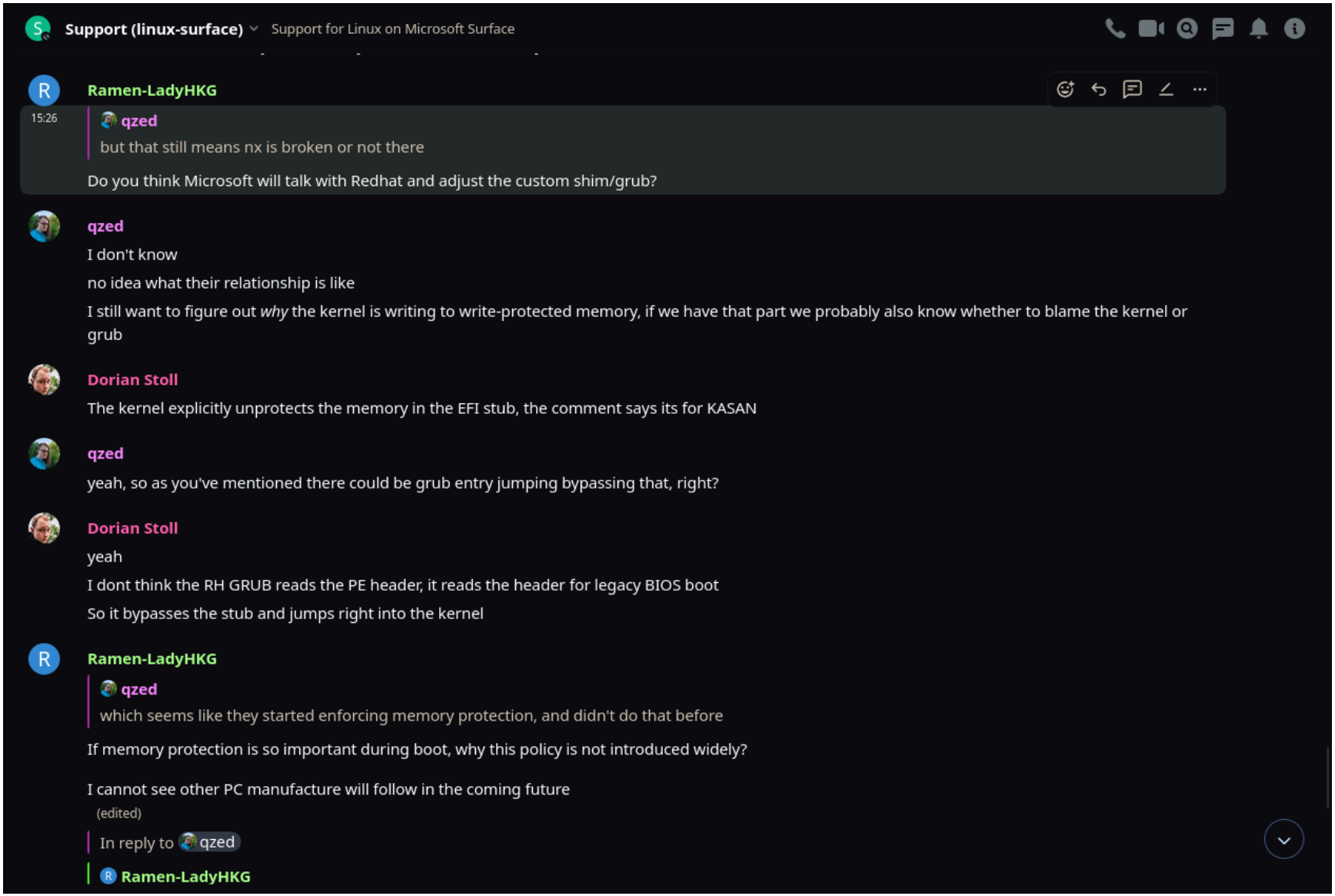

Support (linux-surface)
Support for Linux on Microsoft Surface
Ramen-LadyHKG
19:40
Dorian Stoll
And my guess is that this is the first firmware that actually enforces this NX security option
maybe one day Red Hat will use a more upstreamed version of Grub, and it will work again?
Dorian Stoll
And my guess is that this is the first firmware that actually enforces this NX security option
Because I think these firmware patches will be pushed to newer Surface, like SP9 or so one day.
One day, this issue will happen on those machines.
(edited)
Tue, Jul 18 2023
tajo48 changed their profile picture
qzed
In reply to qzed
Ramen-LadyHKG
Hey qzed , @Dorian Stoll
Do you mind that I quote some of the chats here and show them to Microsoft Support when I have the meeting with them?...
Not at all, go for it. Call me if needed I try to be available
But no promises

[Thu, Jul 27 2023]


Support (linux-surface)
Support for Linux on Microsoft Surface
Thu, Jul 27 2023
Janik (they/them) (es/ihr) changed their display name to Janik (they/them)
alexandermars
I just installed Nobara Linux on my SP6, and I gotta say with a pre-installed surface Linux kernel patch it was hands down the smoothest experience I've ever had installing Linux. I'm pretty sure my toddler could run the installation. (edited)
Ramen-LadyHKG
Ramen-LadyHKG
Due to personal reason, the date of my meeting with Microsoft is shifted.
...
[RIGHT NOW]
If you're interested to attend our meeting with Microsoft Support.
We're going to discuss about the UEFI not booting Linux Problem.
You can join us here:
ID: 265 471 509 06
Passcord: sS8z6b
https://teams.microsoft.com/
(edited)
checking your credentials..
Ramen-LadyHKG
In reply to Ramen-LadyHKG
Ramen-LadyHKG
[RIGHT NOW]
If you're interested to attend our meeting with Microsoft Support....
I've just finished the meeting with Microsoft.
The experience was great.
Send a message...


Support (linux-surface)
Support for Linux on Microsoft Surface
Ramen-LadyHKG
15:14
In reply to Ramen-LadyHKG
Ramen-LadyHKG
[RIGHT NOW]
If you're interested to attend our meeting with Microsoft Support....
I've just finished the meeting with Microsoft.
The experience was great.
A Surface engineer was there as well, he said they'll look into it once the information are gathered.
In reply to Ramen-LadyHKG
Ramen-LadyHKG
I've just finished the meeting with Microsoft.
The experience was great....
As for now, they request some documentations referring to this issue. (like a video footage of the whole process, code or anything that shows what's working and what's not.
They also want to know, what devices are having the problem.
AFAIK, Surface Book2, Pro 5,6 has this problem
Normal:
1 SB2 - 392.178.768.0
2 Pro5/6 - 239.645.768.0
Abnormal:
1 SB2 - 394.651.768.0
2 Pro 5/6 - 238.167.768.0
(edited)


Support (linux-surface)
Support for Linux on Microsoft Surface
(edited)
They'll send me a link to upload all documents that's related to this problem.
(He want me to send a PDF file that gather the UEFI-grub details, chats above) Dorian Stoll qzed
is it ok for you guys?)
In possible future, we'll have another online meeting.
He said that they are welcome other users to join and tell what problems they're having even if it isn't related to this specific UEFI problem.
(edited)
qzed
I think the easiest way to reproduce this is probably installing fedora, right? I.e. fedora/rh patched grub + booting into linux kernel
not sure where I wrote this down, but IIRC modifying the memory allocated for the kernel from rx to rwx (so adding write permissions) does fix it
which seems like they started enforcing memory protection, and didn't do that before
but that still means nx is broken or not there
Ramen-LadyHKG
qzed
I think the easiest way to reproduce this is probably installing fedora, right? I.e. fedora/rh patched grub + booting into linux kernel
Yeah, I was trying to install Fedora right in front of them, they don't seem interest to see.
I just install Fedora on an USB and run in on Surface Pro 5, the result is still the same.
stuck at selecting kernel.
qzed
we'll probably have to address that in the kernel (and maybe grub)
because the kernel really shouldn't try to write to that memory, I think
Ramen-LadyHKG
qzed
but that still means nx is broken or not there
Do you think Microsoft will talk with Redhat and adjust the custom shim/grub?


Support (linux-surface)
Support for Linux on Microsoft Surface
Ramen-LadyHKG
15:26
qzed
but that still means nx is broken or not there
Do you think Microsoft will talk with Redhat and adjust the custom shim/grub?
qzed
I don't know
no idea what their relationship is like
I still want to figure out *why* the kernel is writing to write-protected memory, if we have that part we probably also know whether to blame the kernel or grub
Dorian Stoll
The kernel explicitly unprotects the memory in the EFI stub, the comment says its for KASAN
qzed
yeah, so as you've mentioned there could be grub entry jumping bypassing that, right?
Dorian Stoll
yeah
I dont think the RH GRUB reads the PE header, it reads the header for legacy BIOS boot
So it bypasses the stub and jumps right into the kernel
Ramen-LadyHKG
qzed
which seems like they started enforcing memory protection, and didn't do that before
If memory protection is so important during boot, why this policy is not introduced widely?
I cannot see other PC manufacture will follow in the coming future
(edited)
In reply to qzed
Ramen-LadyHKG

Support (linux-surface) Support for Linux on Microsoft Surface

Ramen-LadyHKG

> **qzed**
> which seems like they started enforcing memory protection, and didn't do that before

If memory protection is so important during boot, why this policy is not introduced widely?

I cannot see other PC manufacture will follow in the coming future
(edited)

> In reply to qzed
>
> **Ramen-LadyHKG**
> If memory protection is so important during boot, why this policy is not introduced widely?
> I cannot see other PC manufacture will follow in the coming future

Since Secure Boot, tpm enforcement on Windows 11 is being blamed right now (edited)

qzed

heh, that's a very good question... the SPX was also pretty much the first UEFI bootable ARM64 device that enforced some kind of memory protection... breaking grub

Dorian Stoll

https://github.com/torvalds/linux/blob/master/drivers/firmware/efi/libstub/x86-stub.c#L296-L322 This is where it modifies the memory permissions

linux/drivers/firmware/efi/libstub/x86-stub.c at master · torvalds/linux - GitHub

Linux kernel source tree. Contribute to torvalds/linux development by creating an account on GitHub.

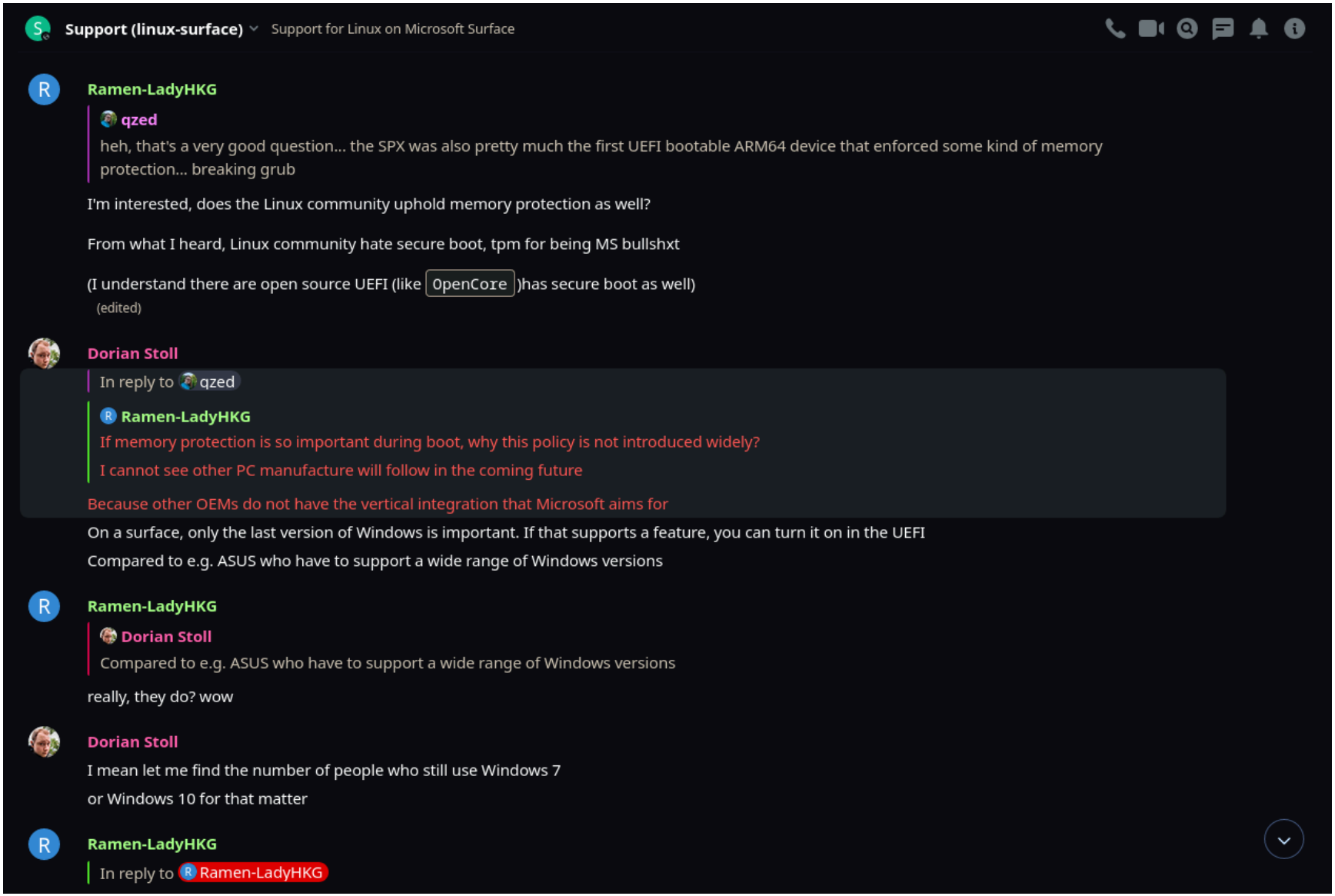
(also I was wrong, nothing about KASAN, its KASLR but only on i686 as it seems.)

Ramen-LadyHKG

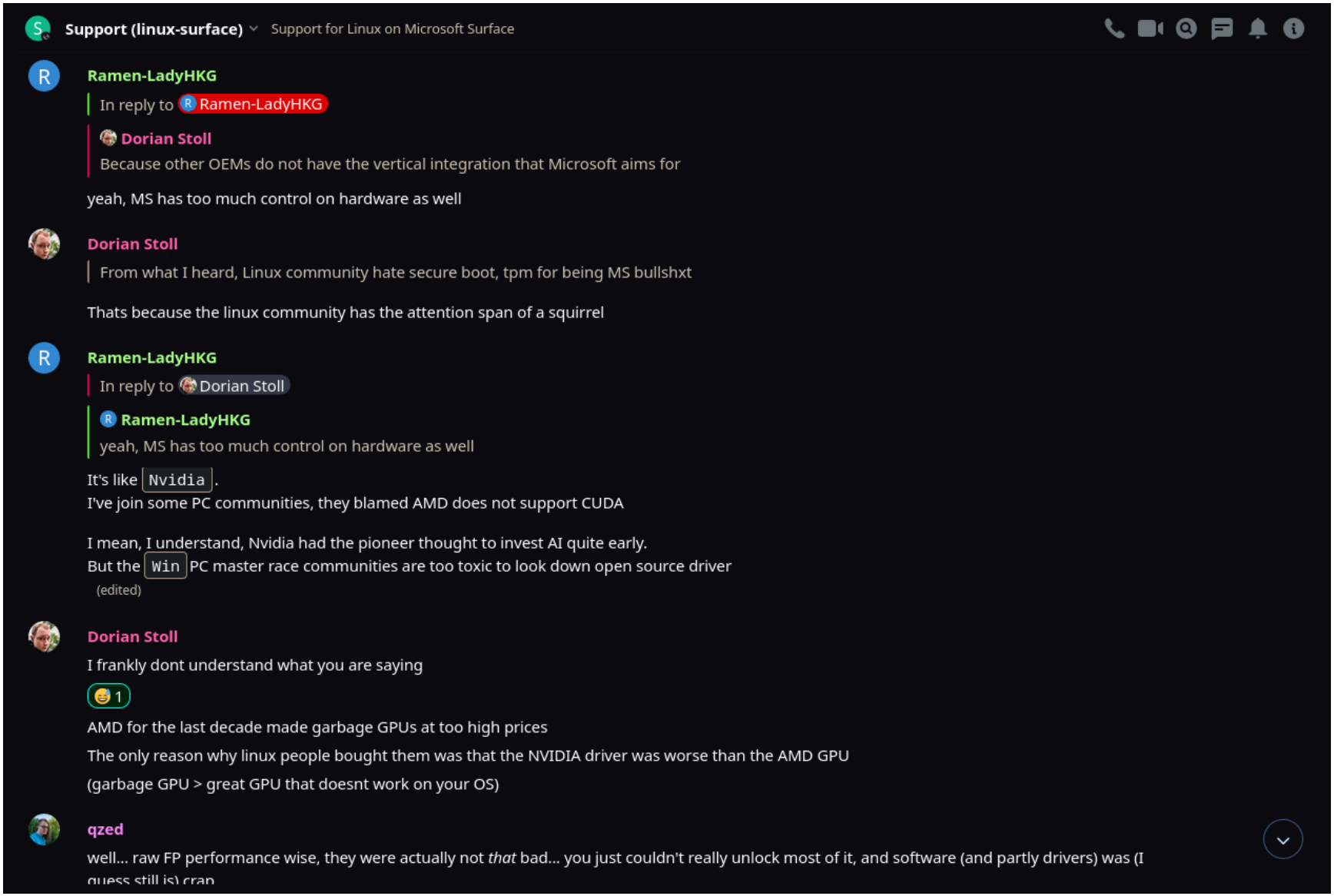
> **qzed**
> heh, that's a very good question... the SPX was also pretty much the first UEFI bootable ARM64 device that enforced some kind of memory protection... breaking grub

I'm interested, does the Linux community uphold memory protection as well?

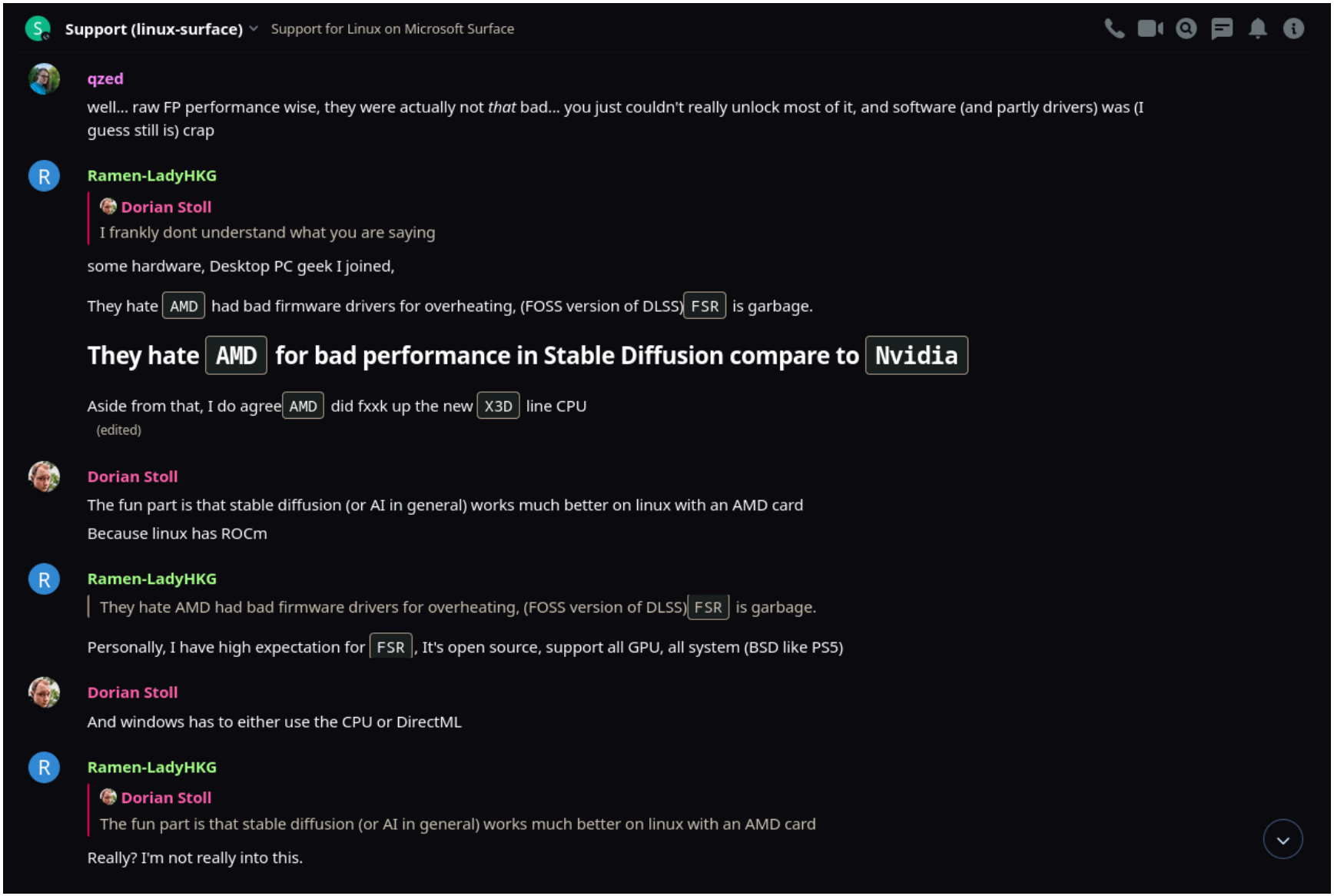
From what I heard, Linux community hate secure boot, tpm for being MS bullshxt


Support (linux-surface)
Support for Linux on Microsoft Surface
Ramen-LadyHKG
qzed
heh, that's a very good question... the SPX was also pretty much the first UEFI bootable ARM64 device that enforced some kind of memory protection... breaking grub
I'm interested, does the Linux community uphold memory protection as well?
From what I heard, Linux community hate secure boot, tpm for being MS bullshxt
(I understand there are open source UEFI (like OpenCore)has secure boot as well)
(edited)
Dorian Stoll
In reply to qzed
Ramen-LadyHKG
If memory protection is so important during boot, why this policy is not introduced widely?
I cannot see other PC manufacture will follow in the coming future
Because other OEMs do not have the vertical integration that Microsoft aims for
On a surface, only the last version of Windows is important. If that supports a feature, you can turn it on in the UEFI
Compared to e.g. ASUS who have to support a wide range of Windows versions
Ramen-LadyHKG
Dorian Stoll
Compared to e.g. ASUS who have to support a wide range of Windows versions
really, they do? wow
Dorian Stoll
I mean let me find the number of people who still use Windows 7
or Windows 10 for that matter
Ramen-LadyHKG
In reply to Ramen-LadyHKG

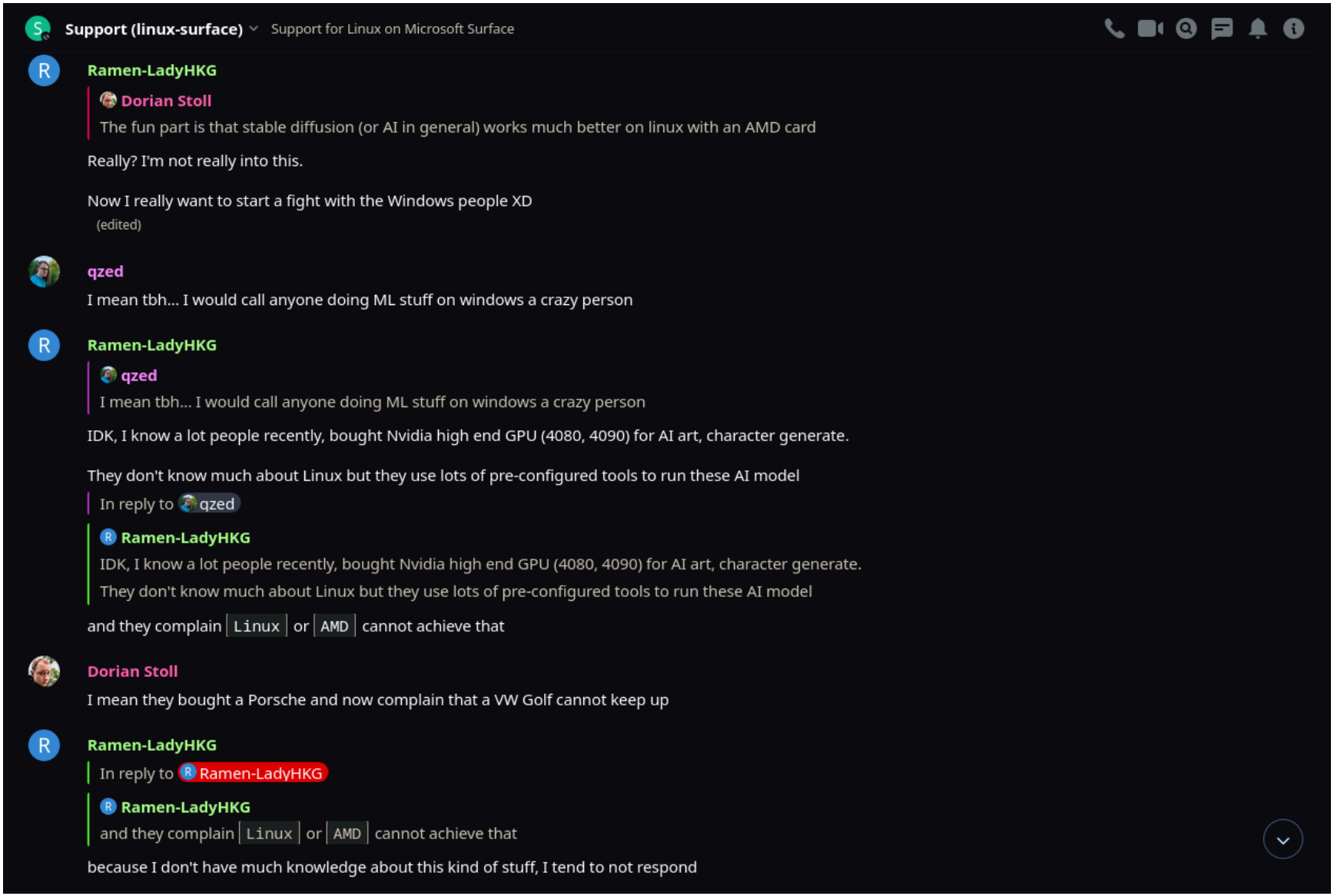
<<<<Skippable>>>> The Next 3 Screenshots are not related<NOT USEFUL>



<<<<Skippable>>>><NOT USEFUL>



<<<<Skippable>>>> <NOT USEFUL>



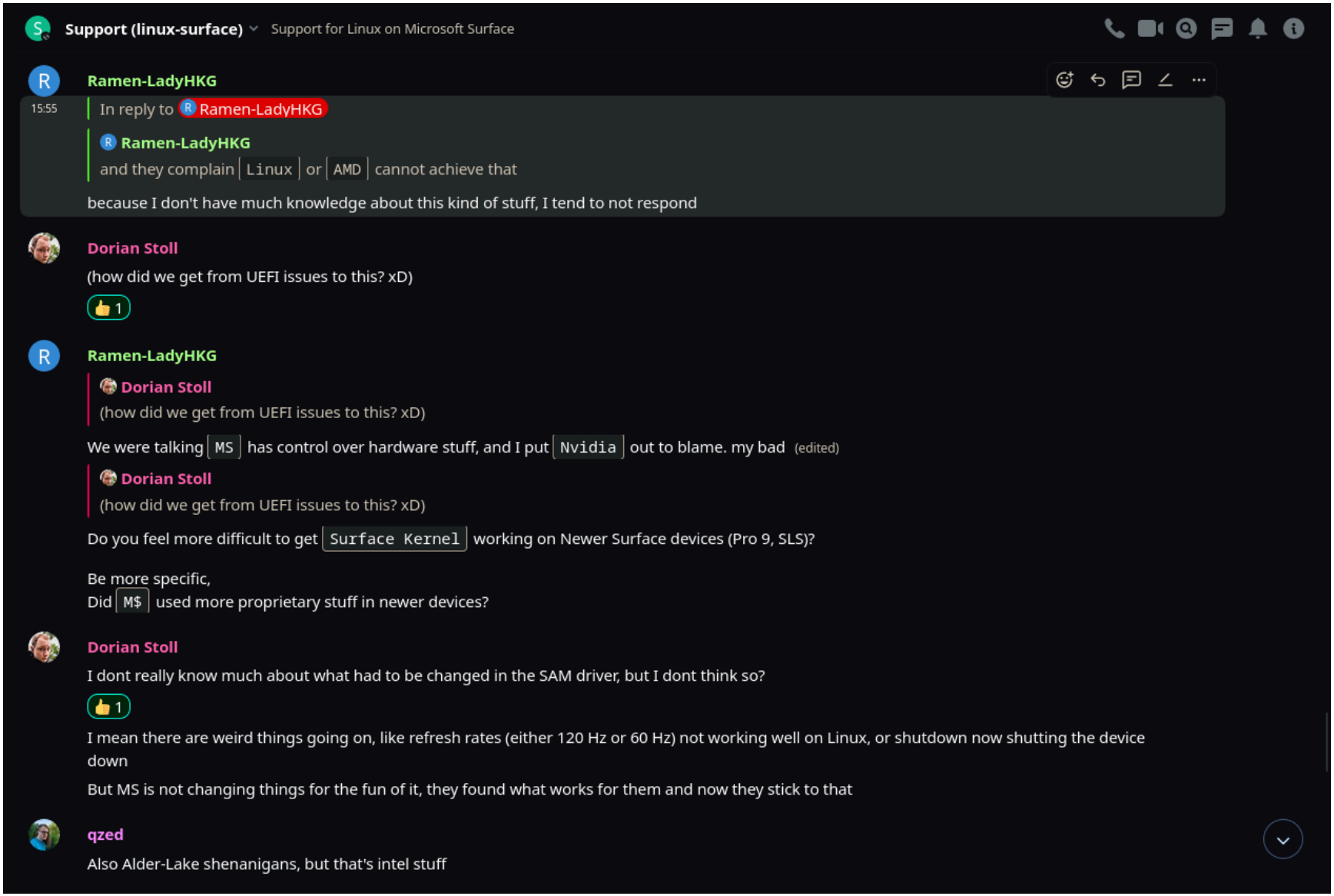
<<<<Skippable>>>> Questions to Linux-Surface Kernel Developers

---

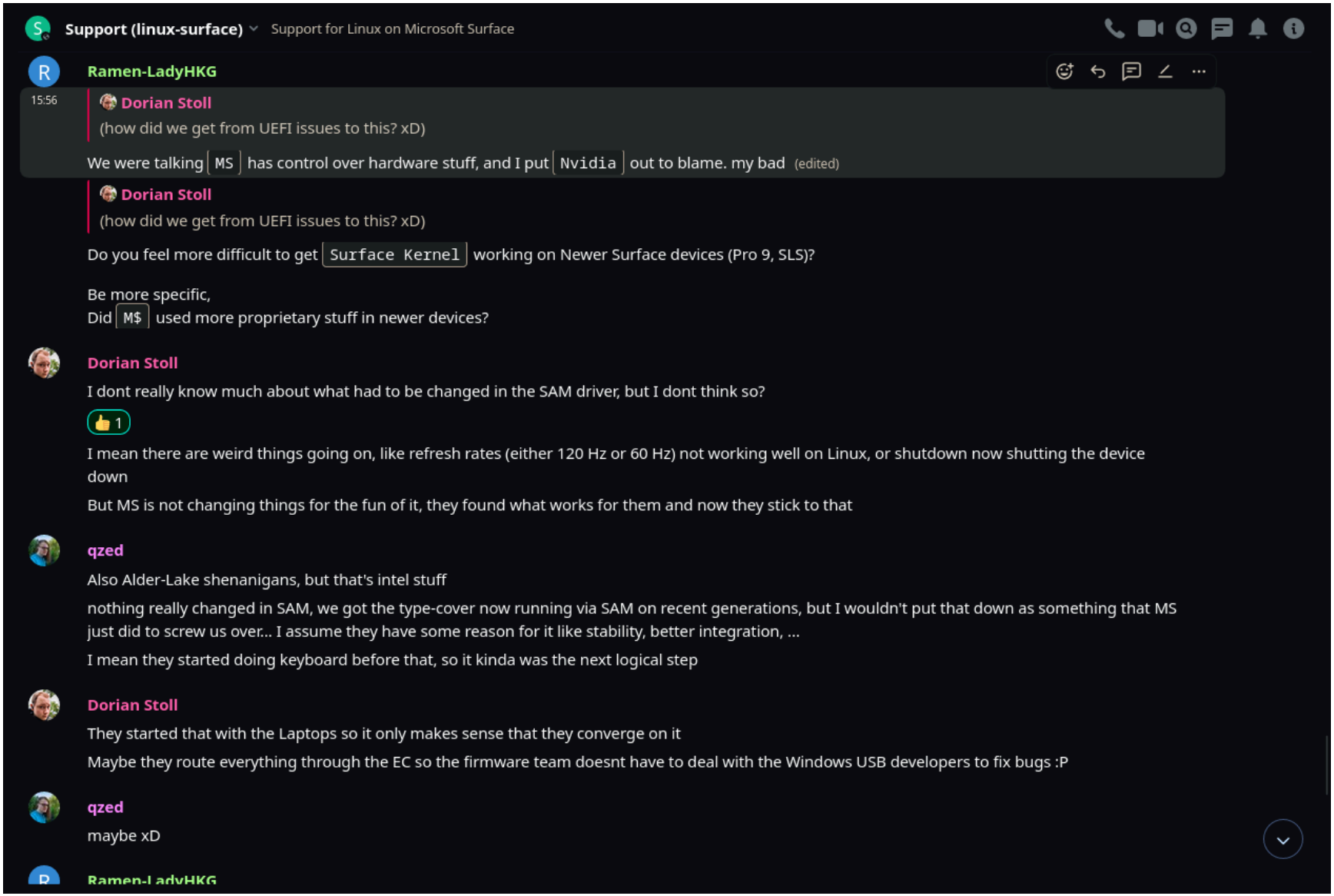
Do you feel it is more difficult to get `Surface Kernel` working on Newer Surface devices (Pro 9, SLS)?

Be more specific,
Did `Microsoft` use more proprietary stuff in newer devices?

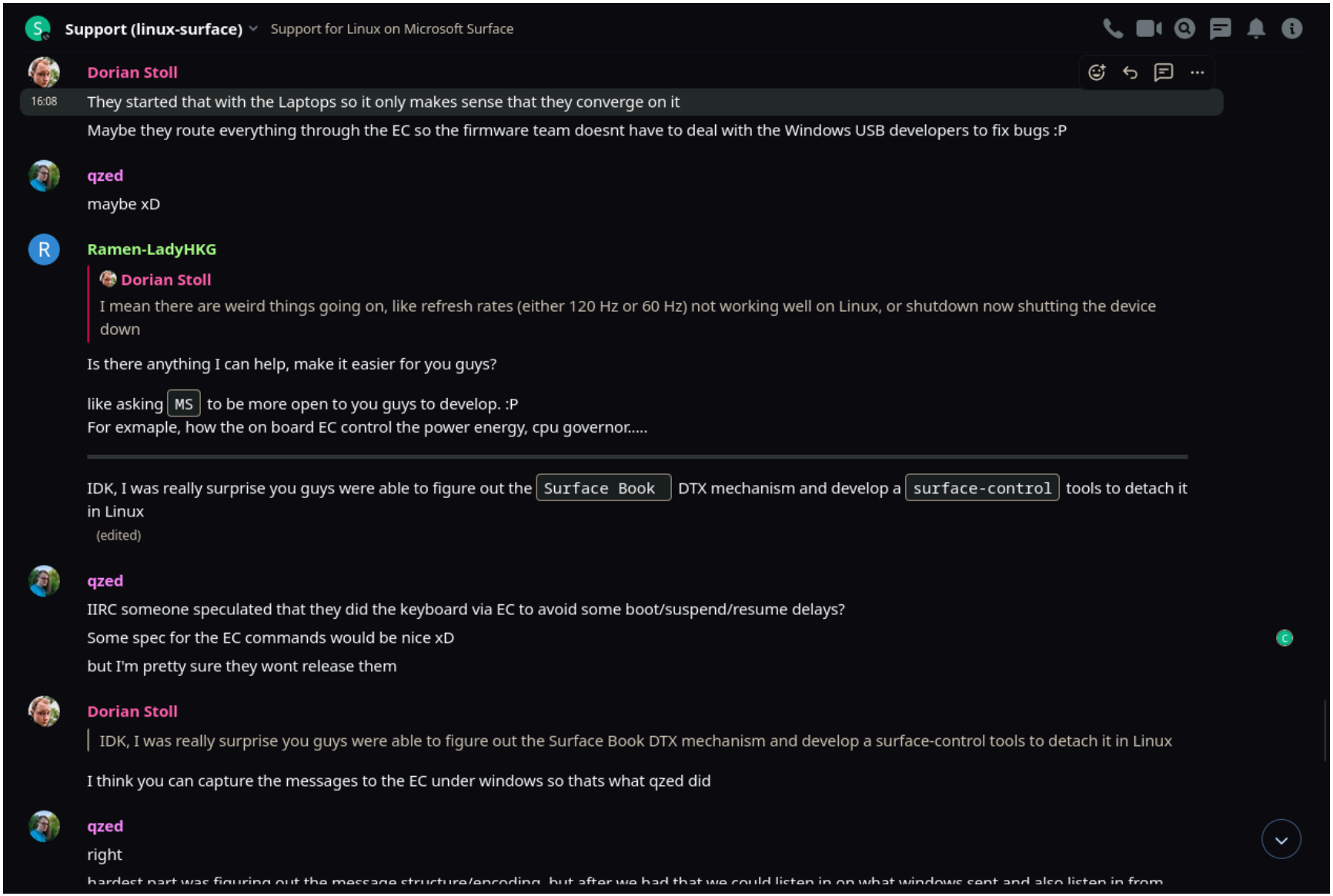
<<<<Skippable>>>><NOT USEFUL>



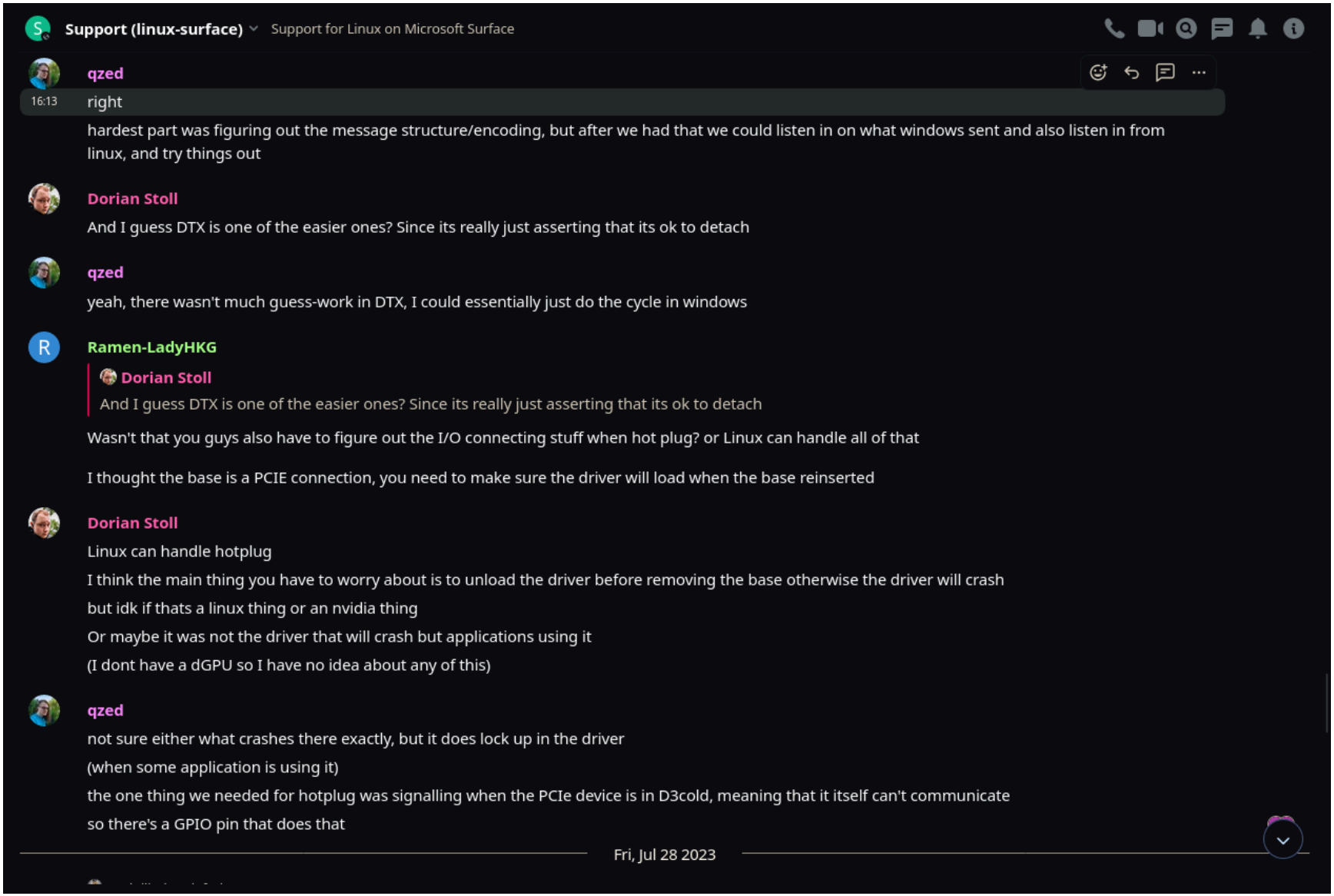
<<<<Skippable>>>><NOT USEFUL>



<<<<Skippable>>>><NOT USEFUL>

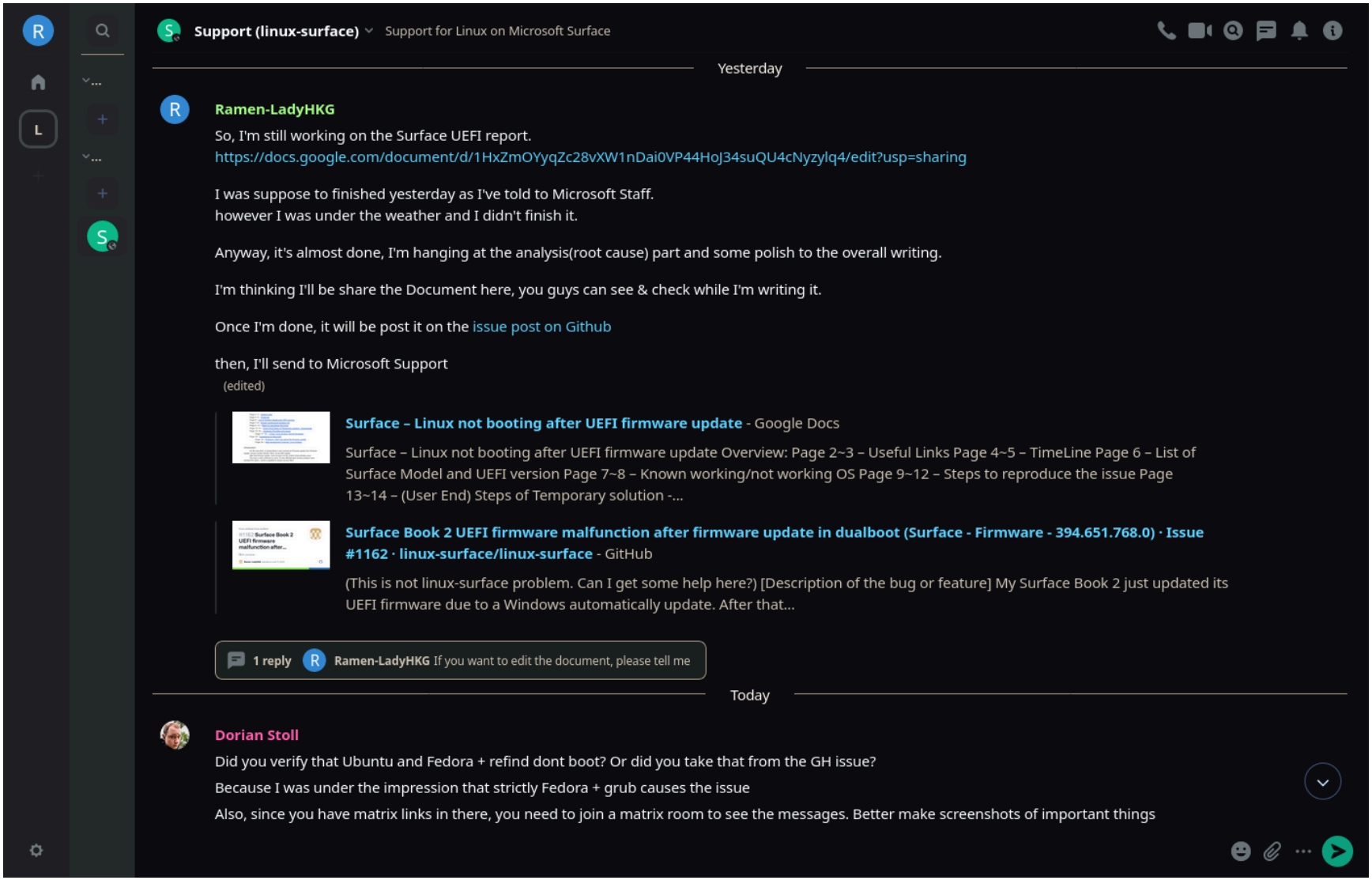


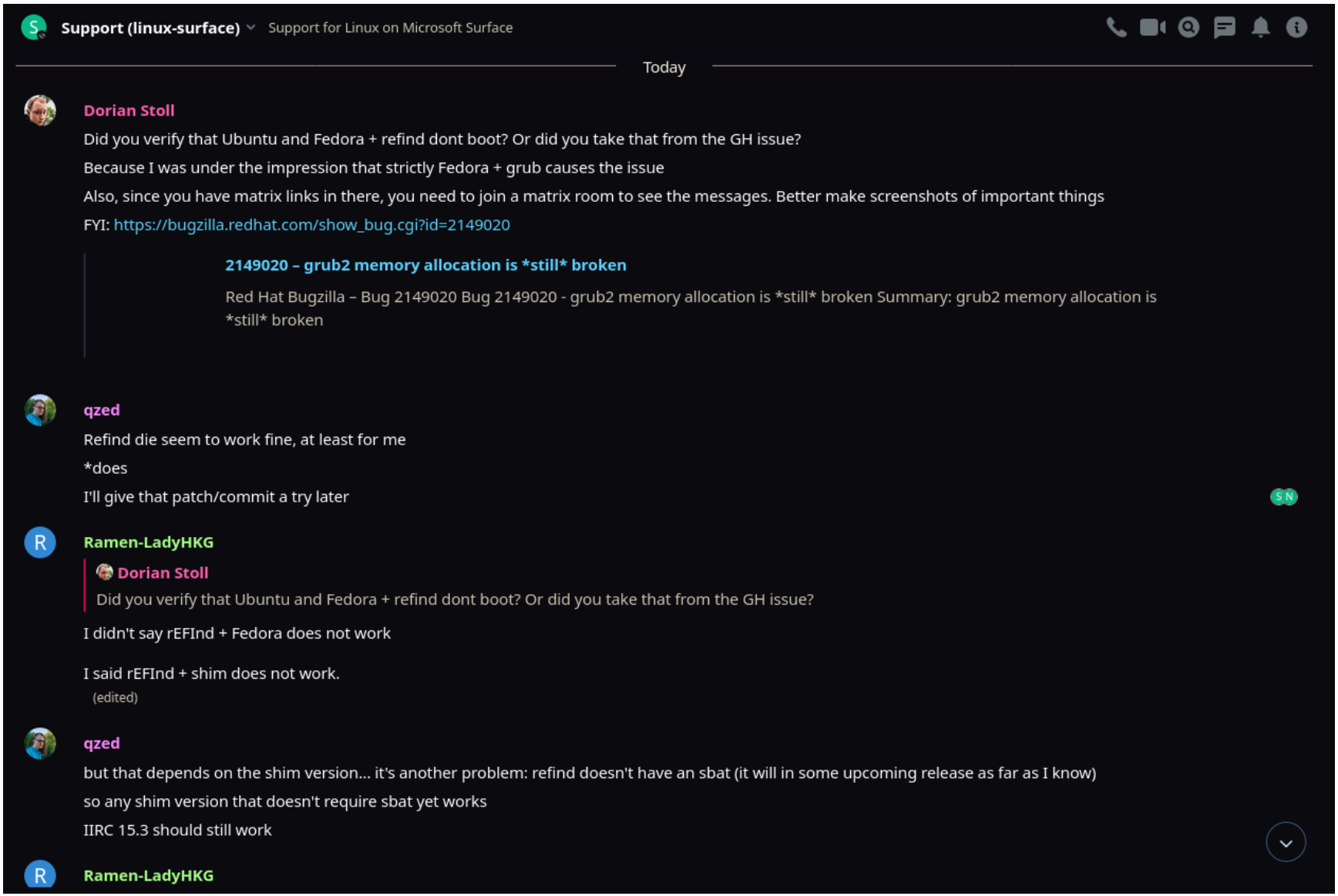
<<<<Skippable>>>><NOT USEFUL>

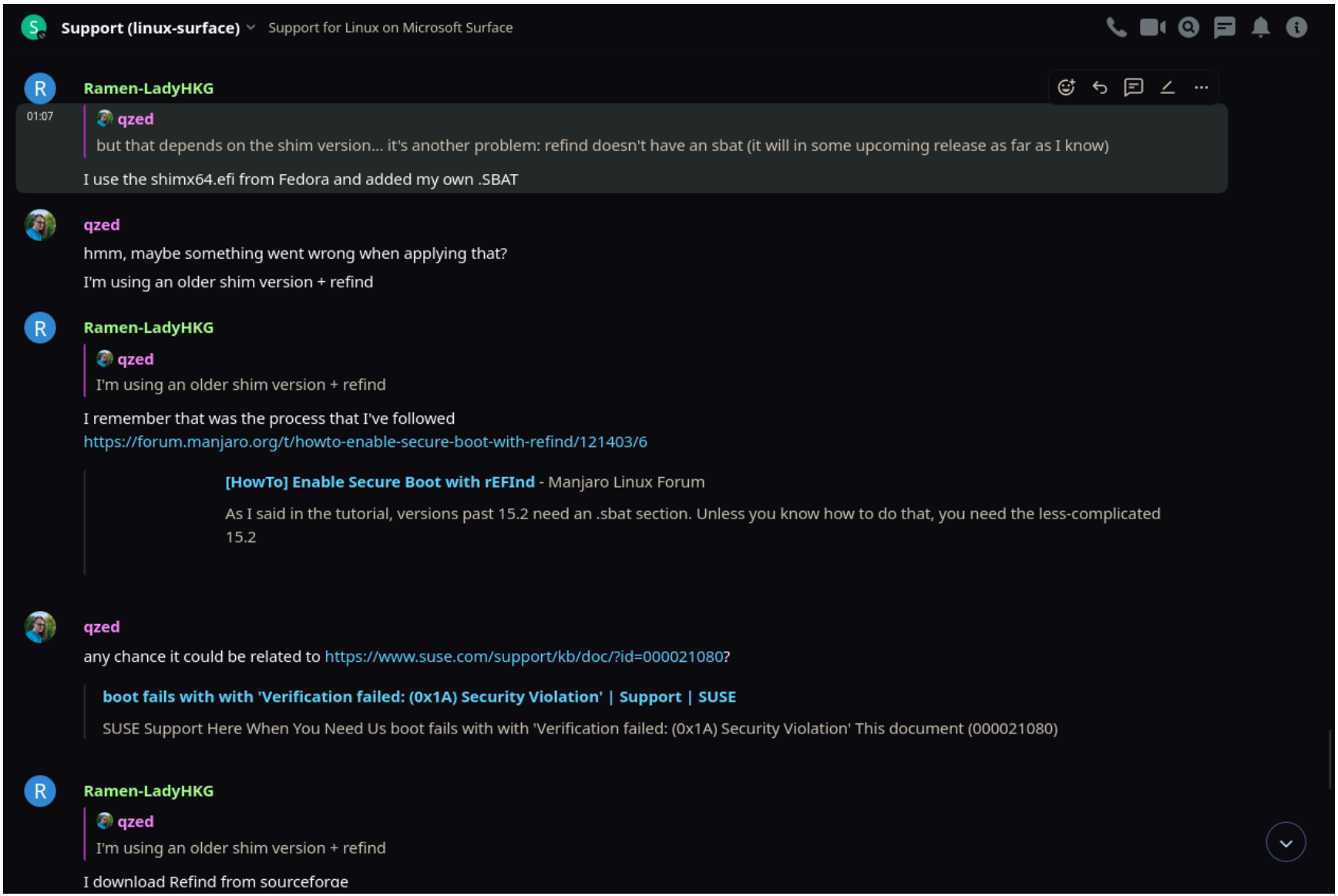


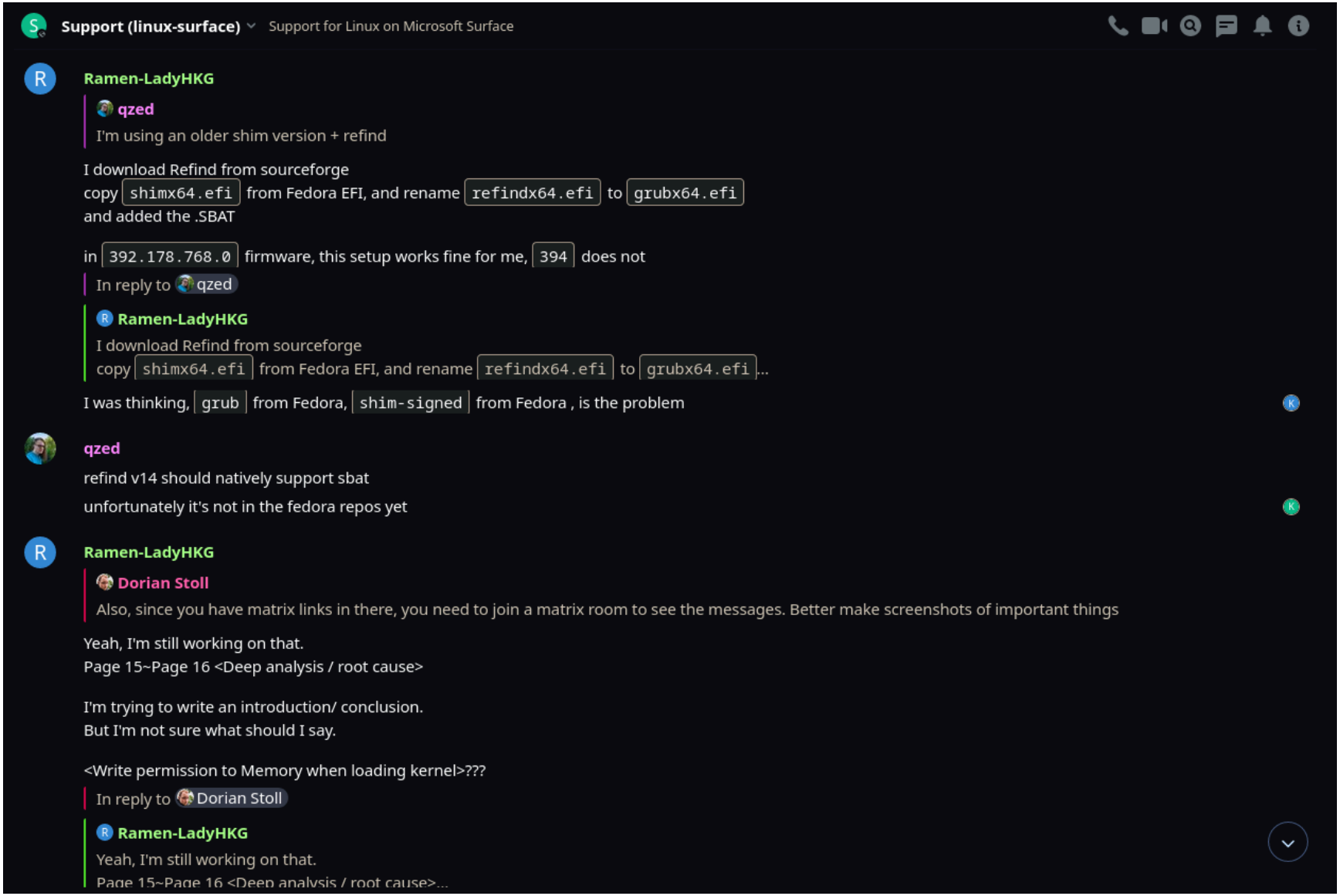
[Sat, Aug 5 2023]

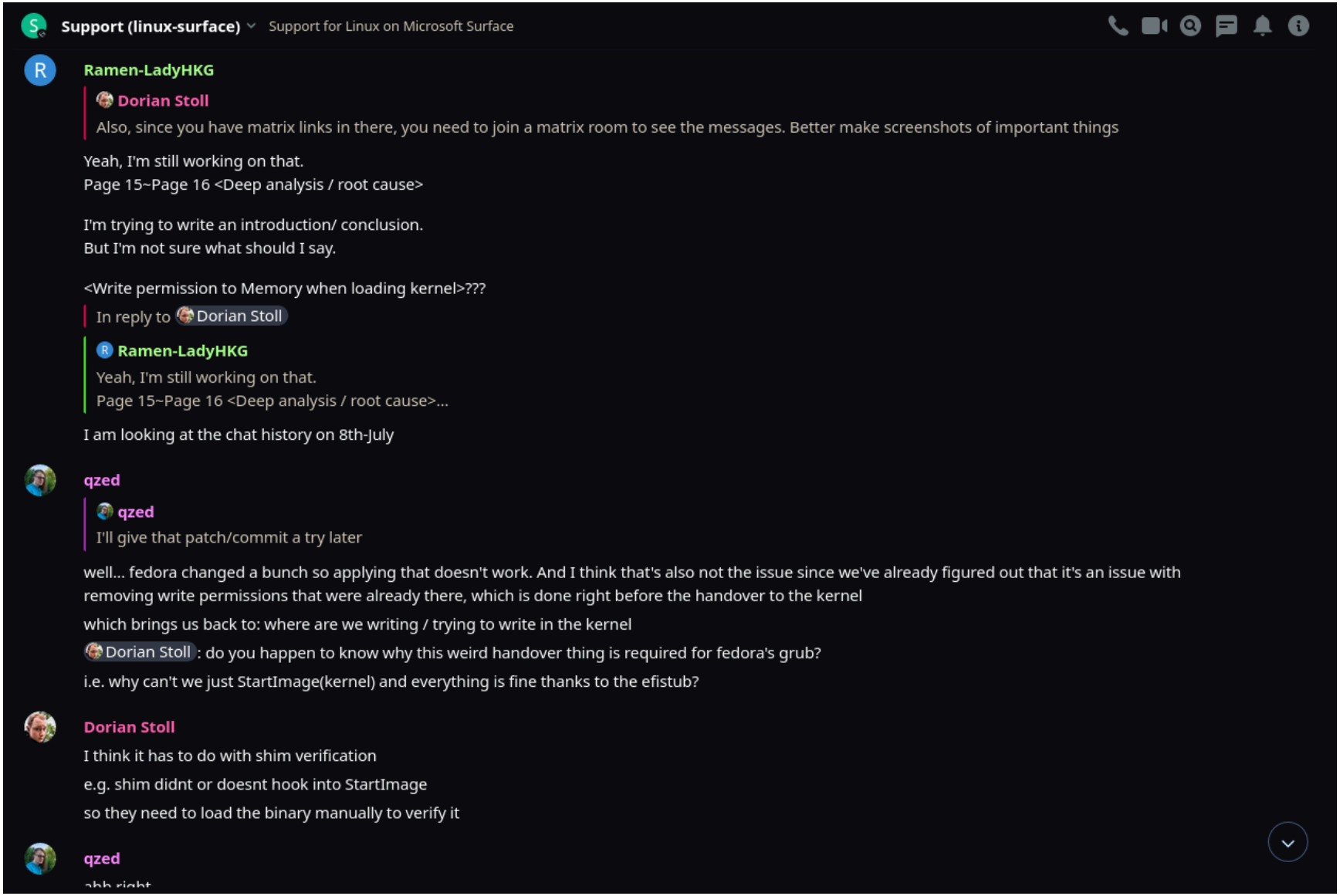
<NOT USEFUL>

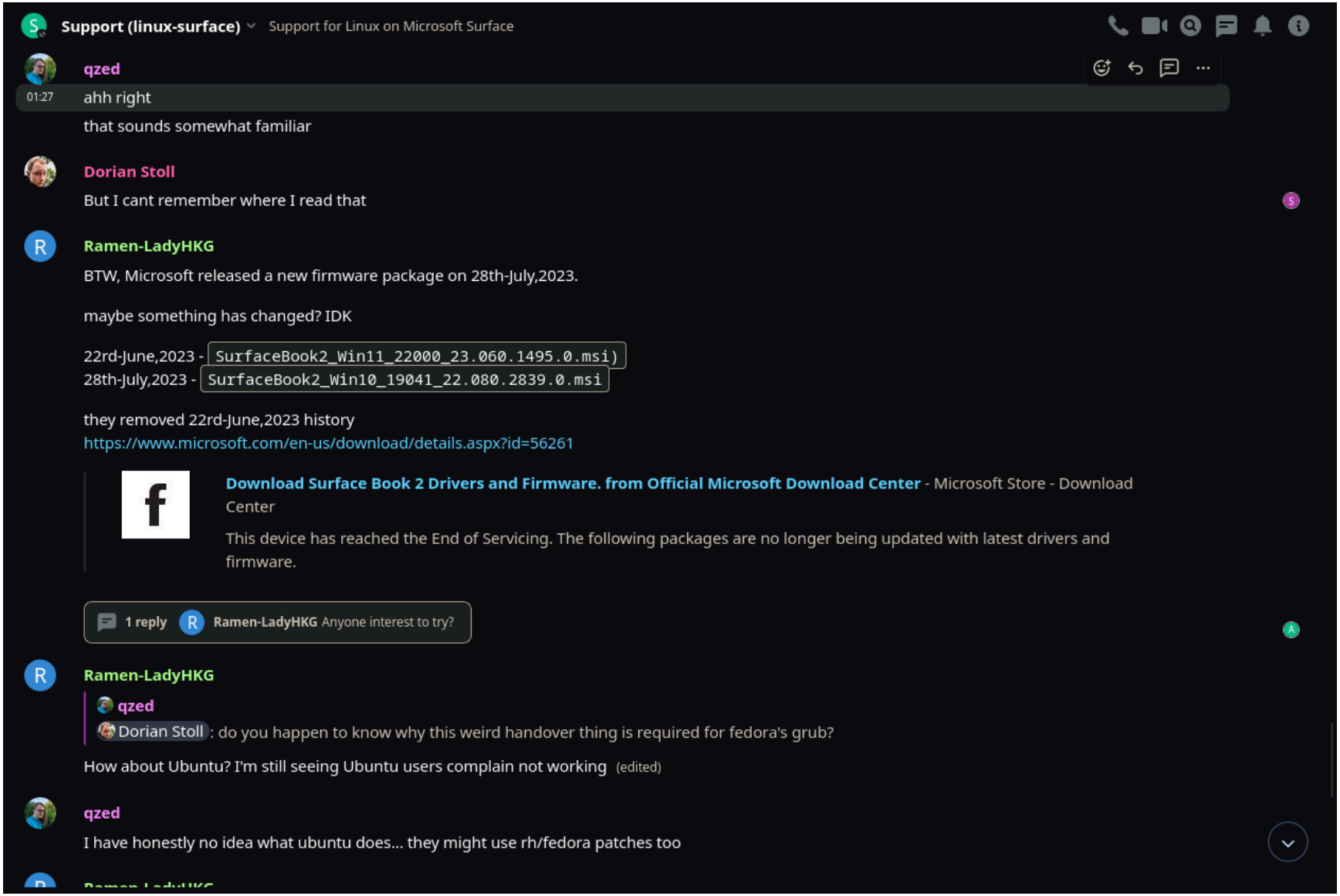

Support (linux-surface)
Support for Linux on Microsoft Surface
Yesterday
Ramen-LadyHKG
So, I'm still working on the Surface UEFI report.
https://docs.google.com/document/d/1HxZmOYyqZc28vXW1nDai0VP44HoJ34suQU4cNyzylq4/edit?usp=sharing
I was suppose to finished yesterday as I've told to Microsoft Staff.
however I was under the weather and I didn't finish it.
Anyway, it's almost done, I'm hanging at the analysis(root cause) part and some polish to the overall writing.
I'm thinking I'll be share the Document here, you guys can see & check while I'm writing it.
Once I'm done, it will be post it on the issue post on Github
then, I'll send to Microsoft Support
(edited)
Surface – Linux not booting after UEFI firmware update - Google Docs
Surface – Linux not booting after UEFI firmware update Overview: Page 2~3 – Useful Links Page 4~5 – TimeLine Page 6 – List of Surface Model and UEFI version Page 7~8 – Known working/not working OS Page 9~12 – Steps to reproduce the issue Page 13~14 – (User End) Steps of Temporary solution -...
Surface Book 2 UEFI firmware malfunction after...
Surface Book 2 UEFI firmware malfunction after firmware update in dualboot (Surface - Firmware - 394.651.768.0) · Issue #1162 · linux-surface/linux-surface - GitHub
(This is not linux-surface problem. Can I get some help here?) [Description of the bug or feature] My Surface Book 2 just updated its UEFI firmware due to a Windows automatically update. After that...
1 reply
Ramen-LadyHKG If you want to edit the document, please tell me
Today
Dorian Stoll
Did you verify that Ubuntu and Fedora + refind dont boot? Or did you take that from the GH issue?
Because I was under the impression that strictly Fedora + grub causes the issue
Also, since you have matrix links in there, you need to join a matrix room to see the messages. Better make screenshots of important things

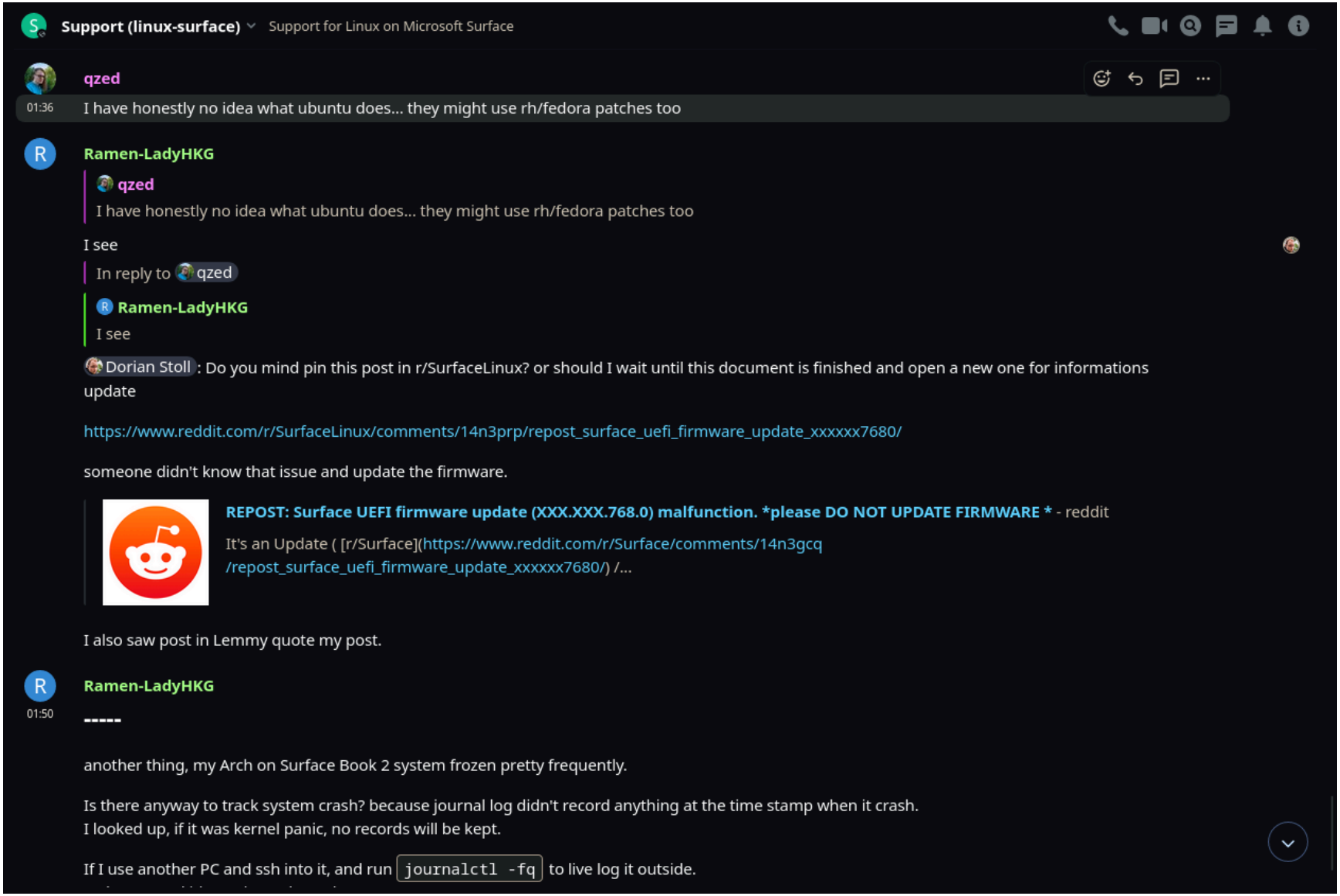

Support (linux-surface)
Support for Linux on Microsoft Surface
Today
Dorian Stoll
Did you verify that Ubuntu and Fedora + refind dont boot? Or did you take that from the GH issue?
Because I was under the impression that strictly Fedora + grub causes the issue
Also, since you have matrix links in there, you need to join a matrix room to see the messages. Better make screenshots of important things
FYI: https://bugzilla.redhat.com/show_bug.cgi?id=2149020
2149020 – grub2 memory allocation is *still* broken
Red Hat Bugzilla – Bug 2149020 Bug 2149020 - grub2 memory allocation is *still* broken Summary: grub2 memory allocation is *still* broken
qzed
Refind die seem to work fine, at least for me
*does
I'll give that patch/commit a try later
Ramen-LadyHKG
Dorian Stoll
Did you verify that Ubuntu and Fedora + refind dont boot? Or did you take that from the GH issue?
I didn't say rEFInd + Fedora does not work
I said rEFInd + shim does not work.
(edited)
qzed
but that depends on the shim version... it's another problem: refind doesn't have an sbat (it will in some upcoming release as far as I know)
so any shim version that doesn't require sbat yet works
IIRC 15.3 should still work
Ramen-LadyHKG


Support (linux-surface)
Support for Linux on Microsoft Surface
Ramen-LadyHKG
01:07
qzed
but that depends on the shim version... it's another problem: refind doesn't have an sbat (it will in some upcoming release as far as I know)
I use the shimx64.efi from Fedora and added my own .SBAT
qzed
hmm, maybe something went wrong when applying that?
I'm using an older shim version + refind
Ramen-LadyHKG
qzed
I'm using an older shim version + refind
I remember that was the process that I've followed
https://forum.manjaro.org/t/howto-enable-secure-boot-with-refind/121403/6
[HowTo] Enable Secure Boot with rEFInd - Manjaro Linux Forum
As I said in the tutorial, versions past 15.2 need an .sbat section. Unless you know how to do that, you need the less-complicated 15.2
qzed
any chance it could be related to https://www.suse.com/support/kb/doc/?id=000021080?
boot fails with with 'Verification failed: (0x1A) Security Violation' | Support | SUSE
SUSE Support Here When You Need Us boot fails with with 'Verification failed: (0x1A) Security Violation' This document (000021080)
Ramen-LadyHKG
qzed
I'm using an older shim version + refind
I download Refind from sourceforge


Support (linux-surface)
Support for Linux on Microsoft Surface
Ramen-LadyHKG
qzed
I'm using an older shim version + refind
I download Refind from sourceforge
copy shimx64.efi from Fedora EFI, and rename refindx64.efi to grubx64.efi
and added the .SBAT
in 392.178.768.0 firmware, this setup works fine for me, 394 does not
In reply to qzed
Ramen-LadyHKG
I download Refind from sourceforge
copy shimx64.efi from Fedora EFI, and rename refindx64.efi to grubx64.efi...
I was thinking, grub from Fedora, shim-signed from Fedora , is the problem
qzed
refind v14 should natively support sbat
unfortunately it's not in the fedora repos yet
Ramen-LadyHKG
Dorian Stoll
Also, since you have matrix links in there, you need to join a matrix room to see the messages. Better make screenshots of important things
Yeah, I'm still working on that.
Page 15~Page 16 <Deep analysis / root cause>
I'm trying to write an introduction/ conclusion.
But I'm not sure what should I say.
<Write permission to Memory when loading kernel>???
In reply to Dorian Stoll
Ramen-LadyHKG
Yeah, I'm still working on that.
Page 15~Page 16 <Deep analysis / root cause>...


Support (linux-surface)
Support for Linux on Microsoft Surface
Ramen-LadyHKG
Dorian Stoll
Also, since you have matrix links in there, you need to join a matrix room to see the messages. Better make screenshots of important things
Yeah, I'm still working on that.
Page 15~Page 16 <Deep analysis / root cause>
I'm trying to write an introduction/ conclusion.
But I'm not sure what should I say.
<Write permission to Memory when loading kernel>???
In reply to Dorian Stoll
Ramen-LadyHKG
Yeah, I'm still working on that.
Page 15~Page 16 <Deep analysis / root cause>...
I am looking at the chat history on 8th-July
qzed
qzed
I'll give that patch/commit a try later
well... fedora changed a bunch so applying that doesn't work. And I think that's also not the issue since we've already figured out that it's an issue with removing write permissions that were already there, which is done right before the handover to the kernel
which brings us back to: where are we writing / trying to write in the kernel
Dorian Stoll : do you happen to know why this weird handover thing is required for fedora's grub?
i.e. why can't we just StartImage(kernel) and everything is fine thanks to the efistub?
Dorian Stoll
I think it has to do with shim verification
e.g. shim didnt or doesnt hook into StartImage
so they need to load the binary manually to verify it
qzed
ahh right

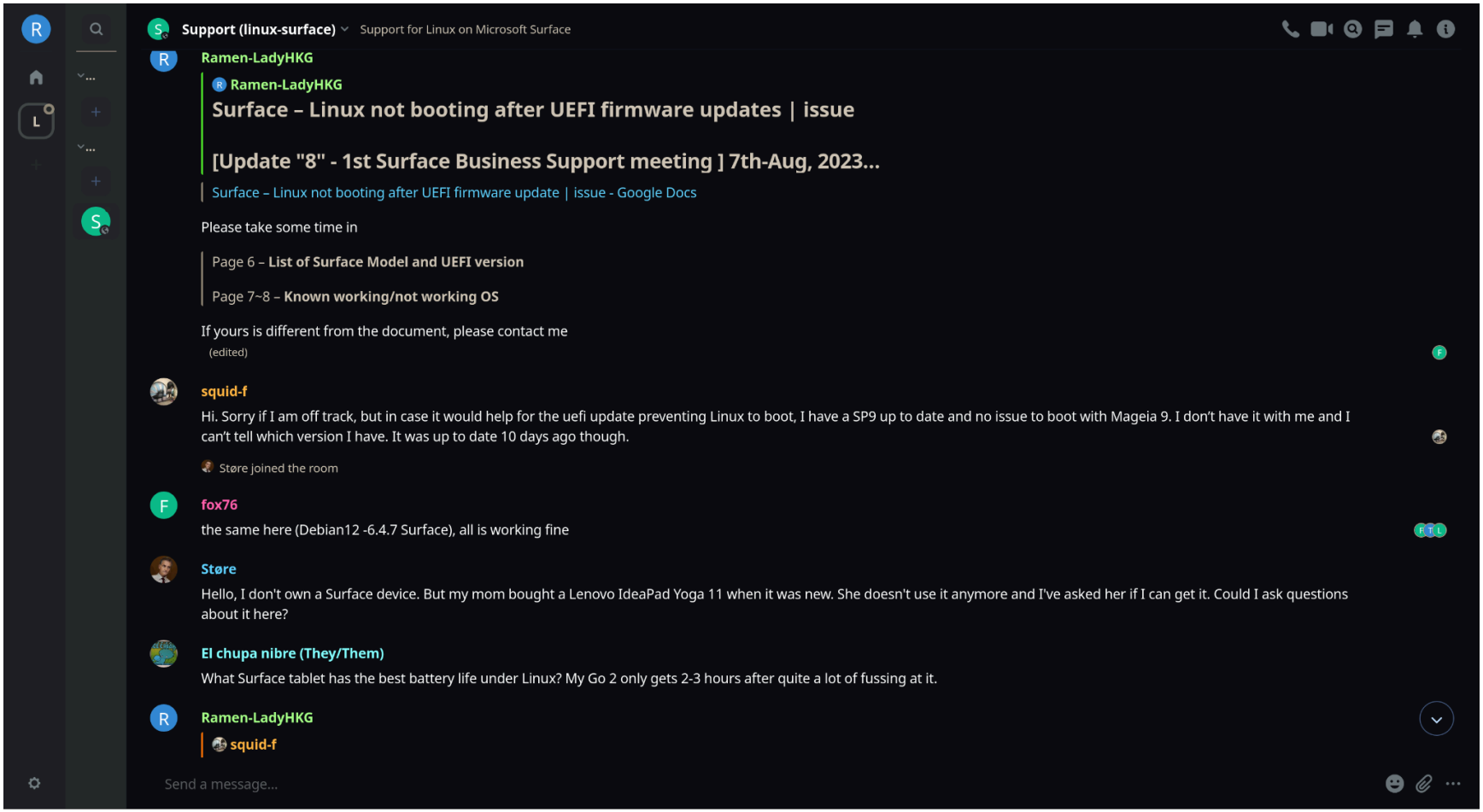

Support (linux-surface)
Support for Linux on Microsoft Surface
qzed
01:27
ahh right
that sounds somewhat familiar
Dorian Stoll
But I cant remember where I read that
Ramen-LadyHKG
BTW, Microsoft released a new firmware package on 28th-July,2023.
maybe something has changed? IDK
22rd-June,2023 - SurfaceBook2_Win11_22000_23.060.1495.0.msi)
28th-July,2023 - SurfaceBook2_Win10_19041_22.080.2839.0.msi
they removed 22rd-June,2023 history
https://www.microsoft.com/en-us/download/details.aspx?id=56261
Download Surface Book 2 Drivers and Firmware. from Official Microsoft Download Center - Microsoft Store - Download Center
This device has reached the End of Servicing. The following packages are no longer being updated with latest drivers and firmware.
1 reply
Ramen-LadyHKG Anyone interest to try?
Ramen-LadyHKG
qzed
Dorian Stoll: do you happen to know why this weird handover thing is required for fedora's grub?
How about Ubuntu? I'm still seeing Ubuntu users complain not working (edited)
qzed
I have honestly no idea what ubuntu does... they might use rh/fedora patches too

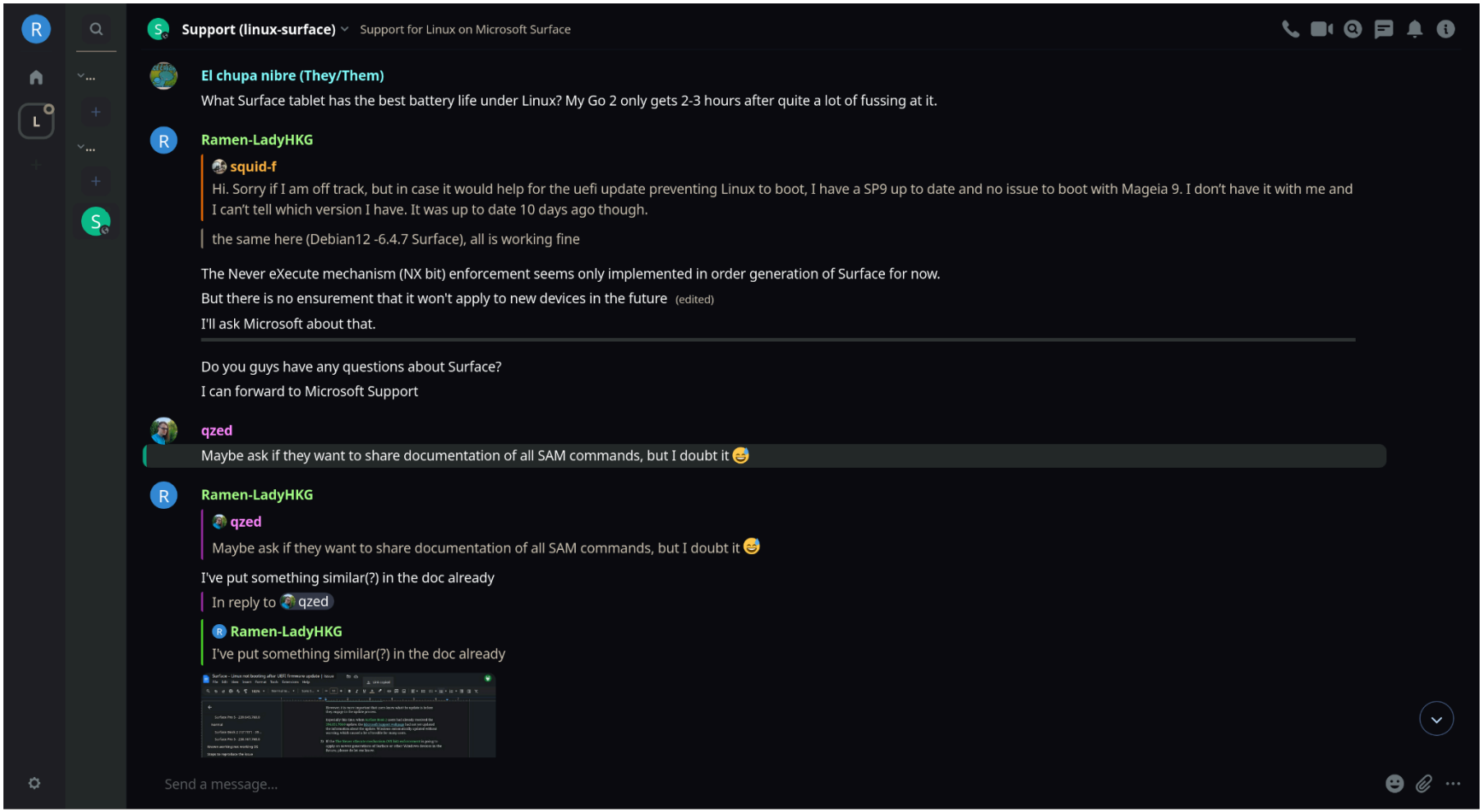

Support (linux-surface)
Support for Linux on Microsoft Surface
qzed
01:36
I have honestly no idea what ubuntu does... they might use rh/fedora patches too
Ramen-LadyHKG
qzed
I have honestly no idea what ubuntu does... they might use rh/fedora patches too
I see
In reply to qzed
Ramen-LadyHKG
I see
Dorian Stoll : Do you mind pin this post in r/SurfaceLinux? or should I wait until this document is finished and open a new one for informations update
https://www.reddit.com/r/SurfaceLinux/comments/14n3prp/repost_surface_uefi_firmware_update_xxxxxx7680/
someone didn't know that issue and update the firmware.
REPOST: Surface UEFI firmware update (XXX.XXX.768.0) malfunction. *please DO NOT UPDATE FIRMWARE * - reddit
It's an Update ([r/Surface](https://www.reddit.com/r/Surface/comments/14n3gcq /repost_surface_uefi_firmware_update_xxxxxx7680/) /...
I also saw post in Lemmy quote my post.
Ramen-LadyHKG
01:50
---
another thing, my Arch on Surface Book 2 system frozen pretty frequently.
Is there anyway to track system crash? because journal log didn't record anything at the time stamp when it crash.
I looked up, if it was kernel panic, no records will be kept.
If I use another PC and ssh into it, and run journalctl -fq to live log it outside.

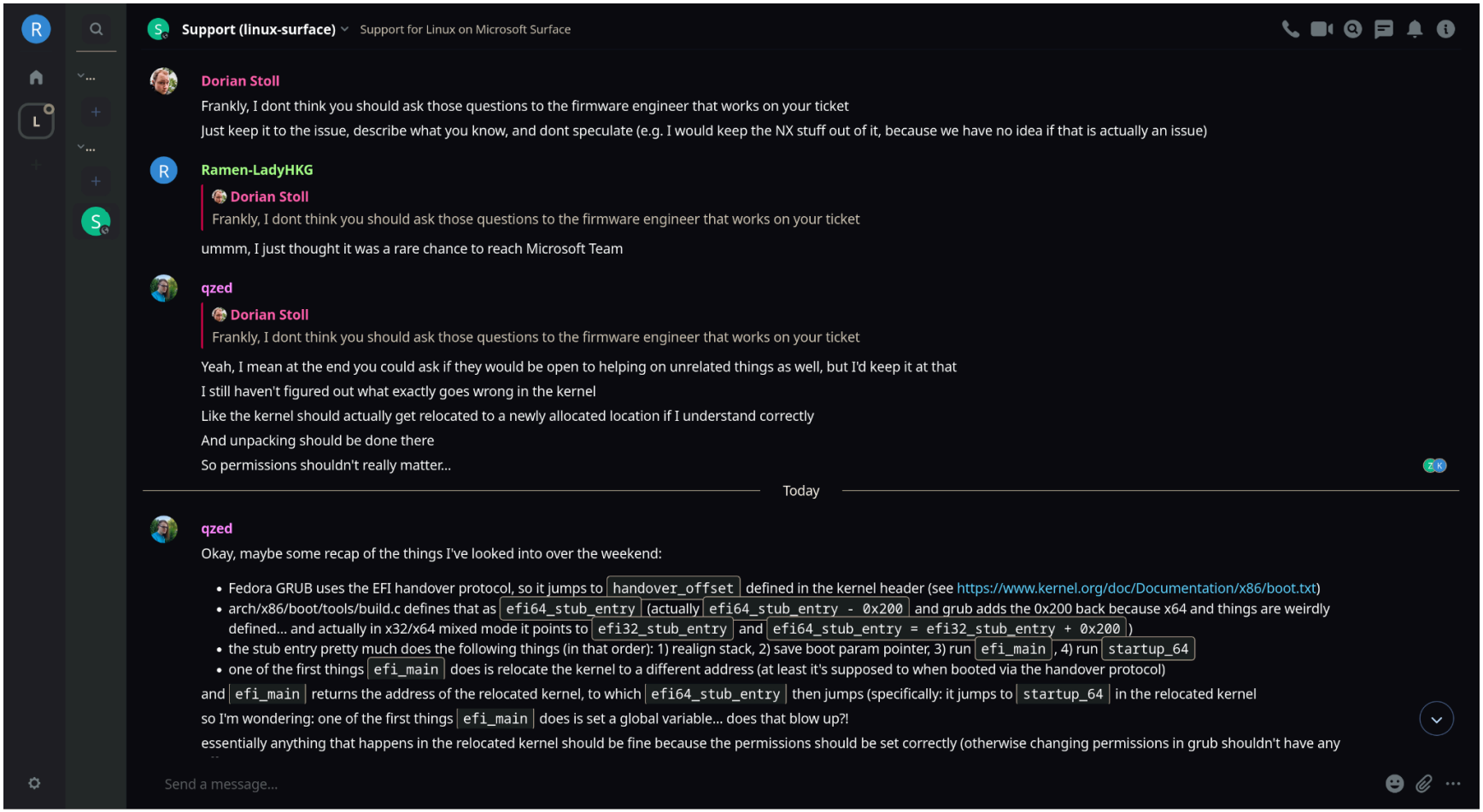
[Mon, Aug 7 2023]

We are not sure if NX stuff is the root cause

“I would keep the NX stuff out of it, because we have no idea if that is actually an issue”


Support (linux-surface)
Support for Linux on Microsoft Surface
Ramen-LadyHKG
Ramen-LadyHKG
Surface – Linux not booting after UEFI firmware updates | issue
[Update "8" - 1st Surface Business Support meeting] 7th-Aug, 2023...
Surface – Linux not booting after UEFI firmware update | issue - Google Docs
Please take some time in
Page 6 – List of Surface Model and UEFI version
Page 7~8 – Known working/not working OS
If yours is different from the document, please contact me
(edited)
squid-f
Hi. Sorry if I am off track, but in case it would help for the uefi update preventing Linux to boot, I have a SP9 up to date and no issue to boot with Mageia 9. I don't have it with me and I can't tell which version I have. It was up to date 10 days ago though.
Støre joined the room
fox76
the same here (Debian12 -6.4.7 Surface), all is working fine
Støre
Hello, I don't own a Surface device. But my mom bought a Lenovo IdeaPad Yoga 11 when it was new. She doesn't use it anymore and I've asked her if I can get it. Could I ask questions about it here?
El chupa nibre (They/Them)
What Surface tablet has the best battery life under Linux? My Go 2 only gets 2-3 hours after quite a lot of fussing at it.
Ramen-LadyHKG
squid-f
Send a message...


Support (linux-surface)
Support for Linux on Microsoft Surface
El chupa nibre (They/Them)
What Surface tablet has the best battery life under Linux? My Go 2 only gets 2-3 hours after quite a lot of fussing at it.
Ramen-LadyHKG
squid-f
Hi. Sorry if I am off track, but in case it would help for the uefi update preventing Linux to boot, I have a SP9 up to date and no issue to boot with Mageia 9. I don't have it with me and I can't tell which version I have. It was up to date 10 days ago though.
the same here (Debian12 -6.4.7 Surface), all is working fine
The Never eXecute mechanism (NX bit) enforcement seems only implemented in order generation of Surface for now.
But there is no ensurement that it won't apply to new devices in the future (edited)
I'll ask Microsoft about that.
Do you guys have any questions about Surface?
I can forward to Microsoft Support
qzed
Maybe ask if they want to share documentation of all SAM commands, but I doubt it
Ramen-LadyHKG
qzed
Maybe ask if they want to share documentation of all SAM commands, but I doubt it
I've put something similar(?) in the doc already
In reply to qzed
Ramen-LadyHKG
I've put something similar(?) in the doc already
Send a message...


Support (linux-surface)
Support for Linux on Microsoft Surface
Dorian Stoll
Frankly, I dont think you should ask those questions to the firmware engineer that works on your ticket
Just keep it to the issue, describe what you know, and dont speculate (e.g. I would keep the NX stuff out of it, because we have no idea if that is actually an issue)
Ramen-LadyHKG
Dorian Stoll
Frankly, I dont think you should ask those questions to the firmware engineer that works on your ticket
ummm, I just thought it was a rare chance to reach Microsoft Team
qzed
Dorian Stoll
Frankly, I dont think you should ask those questions to the firmware engineer that works on your ticket
Yeah, I mean at the end you could ask if they would be open to helping on unrelated things as well, but I'd keep it at that
I still haven't figured out what exactly goes wrong in the kernel
Like the kernel should actually get relocated to a newly allocated location if I understand correctly
And unpacking should be done there
So permissions shouldn't really matter...
Today
qzed
Okay, maybe some recap of the things I've looked into over the weekend:
Fedora GRUB uses the EFI handover protocol, so it jumps to handover_offset defined in the kernel header (see https://www.kernel.org/doc/Documentation/x86/boot.txt)
arch/x86/boot/tools/build.c defines that as efi64_stub_entry (actually efi64_stub_entry - 0x200 and grub adds the 0x200 back because x64 and things are weirdly defined... and actually in x32/x64 mixed mode it points to efi32_stub_entry and efi64_stub_entry = efi32_stub_entry + 0x200)
the stub entry pretty much does the following things (in that order): 1) realign stack, 2) save boot param pointer, 3) run efi_main , 4) run startup_64
one of the first things efi_main does is relocate the kernel to a different address (at least it's supposed to when booted via the handover protocol)
and efi_main returns the address of the relocated kernel, to which efi64_stub_entry then jumps (specifically: it jumps to startup_64 in the relocated kernel
so I'm wondering: one of the first things efi_main does is set a global variable... does that blow up?!
essentially anything that happens in the relocated kernel should be fine because the permissions should be set correctly (otherwise changing permissions in grub shouldn't have any
Send a message...

[Tue, Aug 8 2023]

<USEFUL>

Okay, maybe some recap of the things I've looked into over the weekend:

Okay, maybe some recap of the things I've looked into over the weekend:

- Fedora GRUB uses the EFI handover protocol, so it jumps to `handover_offset` defined in the kernel header (see https://www.kernel.org/doc/Documentation/x86/boot.txt)
- arch/x86/boot/tools/build.c defines that as `efi64_stub_entry` (actually `efi64_stub_entry - 0x200` and grub adds the 0x200 back because x64 and things are weirdly defined... and actually in x32/x64 mixed mode it points to `efi32_stub_entry` and `efi64_stub_entry = efi32_stub_entry + 0x200`)
- the stub entry pretty much does the following things (in that order): 1) realign stack, 2) save boot param pointer, 3) run `efi_main`, 4) run `startup_64`
- one of the first things `efi_main` does is relocate the kernel to a different address (at least it's supposed to when booted via the handover protocol)

and `efi_main` returns the address of the relocated kernel, to which `efi64_stub_entry` then jumps (specifically: it jumps to `startup_64` in the relocated kernel
so I'm wondering: one of the first things `efi_main` does is set a global variable... does that blow up?!
essentially anything that happens in the relocated kernel should be fine because the permissions should be set correctly (otherwise changing permissions in grub shouldn't have any effect)

qzed

Okay, maybe some recap of the things I've looked into over the weekend:

- Fedora GRUB uses the EFI handover protocol, so it jumps to `handover_offset` defined in the kernel header (see https://www.kernel.org/doc/Documentation/x86/boot.txt)
- arch/x86/boot/tools/build.c defines that as `efi64_stub_entry` (actually `efi64_stub_entry - 0x200` and grub adds the 0x200 back because x64 and things are weirdly defined... and actually in x32/x64 mixed mode it points to `efi32_stub_entry` and `efi64_stub_entry = efi32_stub_entry + 0x200`)
- the stub entry pretty much does the following things (in that order): 1) realign stack, 2) save boot param pointer, 3) run `efi_main`, 4) run `startup_64`
- one of the first things `efi_main` does is relocate the kernel to a different address (at least it's supposed to when booted via the handover protocol)

and `efi_main` returns the address of the relocated kernel, to which `efi64_stub_entry` then jumps (specifically: it jumps to `startup_64` in the relocated kernel

so I'm wondering: one of the first things `efi_main` does is set a global variable... does that blow up?!

essentially anything that happens in the relocated kernel should be fine because the permissions should be set correctly (otherwise changing permissions in grub shouldn't have any effect) (edited)

qzed

Message deleted

Dorian Stoll

The RH bugzilla ticket I found a few days ago talks about the heap having to be executable for modules

But idk if it even gets to module loading

qzed

as far as I can tell, the kernel sets up that memory itself

Dorian Stoll

But then why is there an upstream grub commit that has to change the allocation type? (edited)

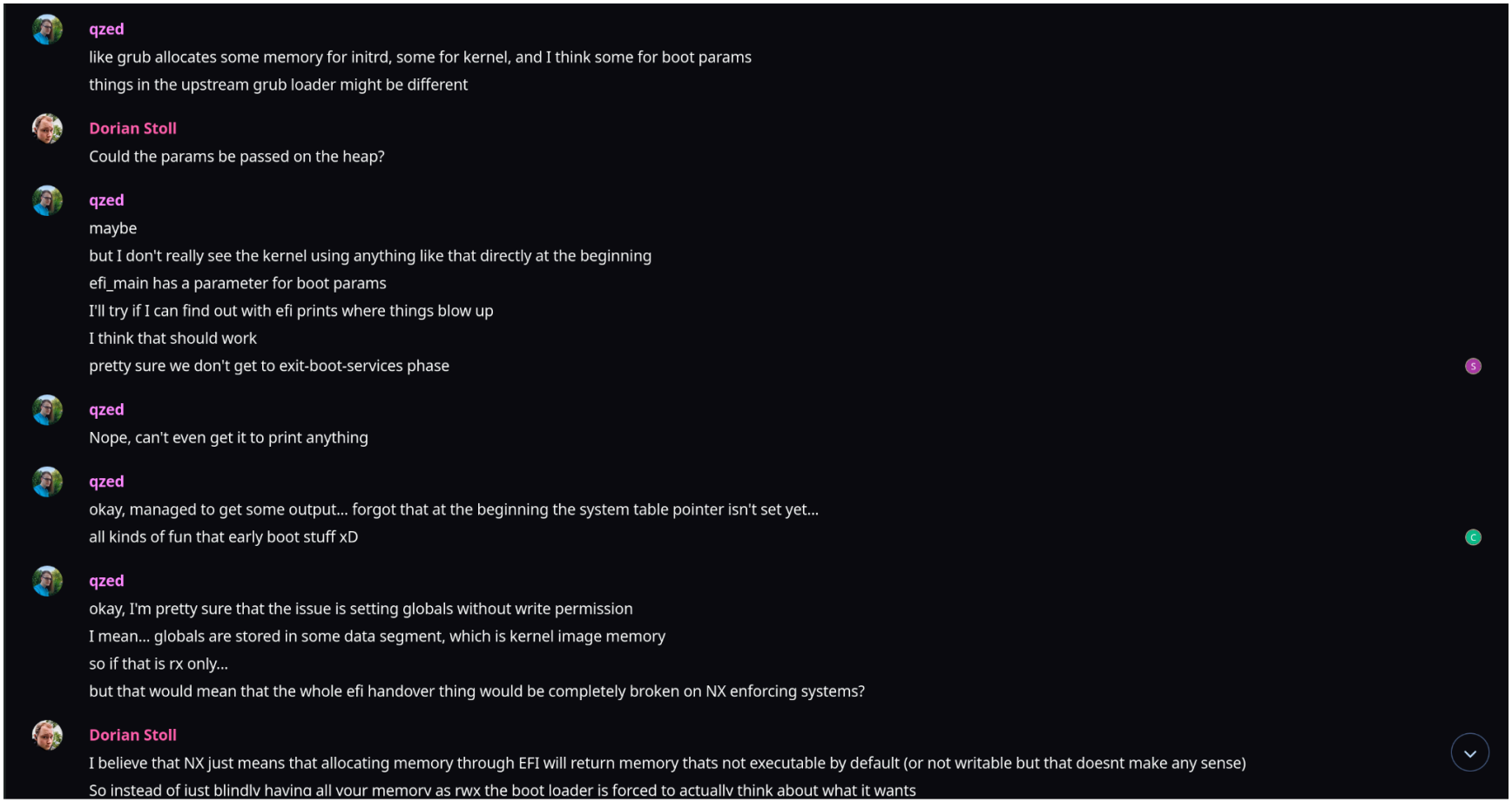
qzed

like grub allocates some memory for initrd, some for kernel, and I think some for boot params

things in the upstream grub loader might be different

Dorian Stoll

Could the params be passed on the heap?



qzed
like grub allocates some memory for initrd, some for kernel, and I think some for boot params
things in the upstream grub loader might be different

Dorian Stoll
Could the params be passed on the heap?

qzed
maybe
but I don't really see the kernel using anything like that directly at the beginning
efi_main has a parameter for boot params
I'll try if I can find out with efi prints where things blow up
I think that should work
pretty sure we don't get to exit-boot-services phase

qzed
Nope, can't even get it to print anything

qzed
okay, managed to get some output... forgot that at the beginning the system table pointer isn't set yet...
all kinds of fun that early boot stuff xD

qzed
okay, I'm pretty sure that the issue is setting globals without write permission
I mean... globals are stored in some data segment, which is kernel image memory
so if that is rx only...
but that would mean that the whole efi handover thing would be completely broken on NX enforcing systems?

Dorian Stoll
I believe that NX just means that allocating memory through EFI will return memory thats not executable by default (or not writable but that doesnt make any sense)
So instead of just blindly having all your memory as rwx the boot loader is forced to actually think about what it wants

qzed
okay, managed to get some output... forgot that at the beginning the system table pointer isn't set yet...
all kinds of fun that early boot stuff xD

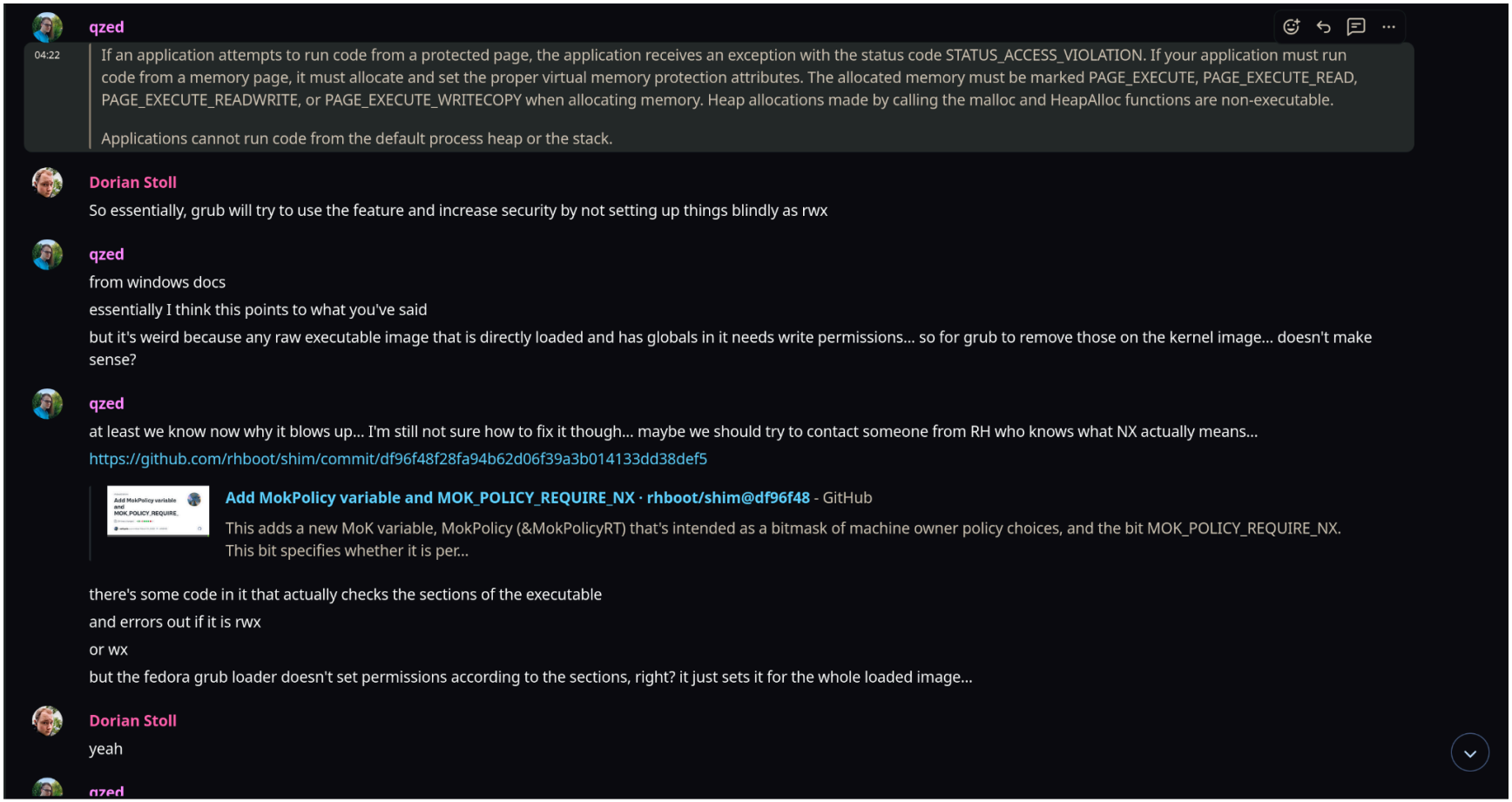
qzed
okay, I'm pretty sure that the issue is setting globals without write permission
I mean... globals are stored in some data segment, which is kernel image memory
so if that is rx only...
but that would mean that the whole efi handover thing would be completely broken on NX enforcing systems?

Dorian Stoll
I believe that NX just means that allocating memory through EFI will return memory thats not executable by default (or not writable but that doesnt make any sense)
So instead of just blindly having all your memory as rwx the boot loader is forced to actually think about what it wants
so that you only have +x where it is actually needed

qzed
I think that would make most sense...
I don't quite understand why grub does this whole permission thing when nx support was detected
or what even "nx support" means
it's a flag in a PE header

Dorian Stoll
I think it means "can deal with allocations that are rw by default"
But not "can deal with getting memory with wrong permissions passed"

qzed
> If an application attempts to run code from a protected page, the application receives an exception with the status code STATUS_ACCESS_VIOLATION. If your application must run code from a memory page, it must allocate and set the proper virtual memory protection attributes. The allocated memory must be marked PAGE_EXECUTE, PAGE_EXECUTE_READ, PAGE_EXECUTE_READWRITE, or PAGE_EXECUTE_WRITECOPY when allocating memory. Heap allocations made by calling the malloc and HeapAlloc functions are non-executable.
>
> Applications cannot run code from the default process heap or the stack.



qzed 04:22

> If an application attempts to run code from a protected page, the application receives an exception with the status code STATUS_ACCESS_VIOLATION. If your application must run code from a memory page, it must allocate and set the proper virtual memory protection attributes. The allocated memory must be marked PAGE_EXECUTE, PAGE_EXECUTE_READ, PAGE_EXECUTE_READWRITE, or PAGE_EXECUTE_WRITECOPY when allocating memory. Heap allocations made by calling the malloc and HeapAlloc functions are non-executable.
>
> Applications cannot run code from the default process heap or the stack.

Dorian Stoll

So essentially, grub will try to use the feature and increase security by not setting up things blindly as rwx

qzed

from windows docs

essentially I think this points to what you've said

but it's weird because any raw executable image that is directly loaded and has globals in it needs write permissions... so for grub to remove those on the kernel image... doesn't make sense?

qzed

at least we know now why it blows up... I'm still not sure how to fix it though... maybe we should try to contact someone from RH who knows what NX actually means...

https://github.com/rhboot/shim/commit/df96f48f28fa94b62d06f39a3b014133dd38def5

> **Add MokPolicy variable and MOK_POLICY_REQUIRE_NX · rhboot/shim@df96f48** - GitHub
>
> This adds a new MoK variable, MokPolicy (&MokPolicyRT) that's intended as a bitmask of machine owner policy choices, and the bit MOK_POLICY_REQUIRE_NX. This bit specifies whether it is per...

there's some code in it that actually checks the sections of the executable

and errors out if it is rwx

or wx

but the fedora grub loader doesn't set permissions according to the sections, right? it just sets it for the whole loaded image...

Dorian Stoll

yeah

qzed

from windows docs

essentially I think this points to what you've said

but it's weird because any raw executable image that is directly loaded and has globals in it needs write permissions... so for grub to remove those on the kernel image... doesn't make sense?

qzed

at least we know now why it blows up... I'm still not sure how to fix it though... maybe we should try to contact someone from RH who knows what NX actually means...

https://github.com/rhboot/shim/commit/df96f48f28fa94b62d06f39a3b014133dd38def5

Add MokPolicy variable and MOK_POLICY_REQUIRE_NX · rhboot/shim@df96f48 - GitHub

This adds a new MoK variable, MokPolicy (&MokPolicyRT) that's intended as a bitmask of machine owner policy choices, and the bit MOK_POLICY_REQUIRE_NX. This bit specifies whether it is per...

there's some code in it that actually checks the sections of the executable

and errors out if it is rwx

or wx

but the fedora grub loader doesn't set permissions according to the sections, right? it just sets it for the whole loaded image...

Dorian Stoll

yeah

qzed

so that's broken...

the image itself might as well be compatible

yay custom loader code...

Dorian Stoll

Is the kernel actually a proper ELF or PE binary with sections? (I assume the PE header is just a header to make the UEFI jump to the entry point)

qzed

04:39 I'm wondering that as well... I assume not

+6