

# How To Protect Your Server Against the Meltdown and Spectre Vulnerabilities



Posted January 10, 2018  146.8k SECURITY

By: Justin Ellingwood

## What are Meltdown and Spectre?

On January 4, 2018, multiple vulnerabilities in the design of modern CPUs were disclosed. Taking advantage of certain processor performance optimizations, these vulnerabilities—named **Meltdown** and **Spectre**—make it possible for attackers to coerce applications into revealing the contents of system and application memory when manipulated correctly. These attacks work because the normal privileges checking behavior within the processor is subverted through the interaction of features like speculative execution, branch prediction, out-of-order execution, and caching.

Meltdown was disclosed in [CVE-2017-5754](#). Spectre was disclosed in [CVE-2017-5753](#) and [CVE-2017-5715](#).

For more detailed information, check out the [how does meltdown work?](#) and [how does spectre work?](#) sections below.

## Am I Affected by Meltdown and Spectre?

Meltdown and Spectre affect the majority of modern processors. The processor optimizations that are used in these vulnerabilities are a core design feature of most CPUs, meaning that most systems are vulnerable until specifically patched. This includes desktop computers, servers, and compute instances operating in Cloud environments.

Patches to protect against Meltdown are being released from operating system vendors. While updates are also being released for Spectre, it represents an entire class of vulnerabilities, so it will likely require more extensive ongoing remediation.

In cloud and virtualized environments, providers will need to update the underlying infrastructure to protect their guests. Users will need to update their servers to mitigate the impact within guest operating systems.

## How Can I Protect Myself?

Full protection against this class of vulnerability will likely require changes in CPU design. In the interim, software updates can provide mitigation against exploits by disabling or working around some of the optimized behavior that leads to these vulnerabilities.

Unfortunately, because these patches affect the optimization routines within the processor, mitigation patches may decrease the performance of your server. The extent of the slowdown is highly dependent on the type of work being performed, with I/O intensive processes experiencing the largest impact.

## Current Mitigation Patch Status

At the time of writing (January 9, 2018), Linux distributions have started to distribute patches, but no distributions are yet fully patched.

Distributions that have released kernel updates with **partial mitigation** (patched for Meltdown **AND** variant 1 of Spectre) include:

- CentOS 7: kernel 3.10.0-693.11.6
- CentOS 6: kernel 2.6.32-696.18.7

Distributions that have released kernel updates with **partial mitigation** (patched for Meltdown) include:

- Fedora 27: kernel 4.14.11-300
- Fedora 26: kernel 4.14.11-200
- Ubuntu 17.10: kernel 4.13.0-25-generic
- Ubuntu 16.04: kernel 4.4.0-109-generic
- Ubuntu 14.04: kernel 3.13.0-139-generic
- Debian 9: kernel 4.9.0-5-amd64
- Debian 8: kernel 3.16.0-5-amd64
- Debian 7: kernel 3.2.0-5-amd64
- Fedora 27 Atomic: kernel 4.14.11-300.fc27.x86\_64
- CoreOS: kernel 4.14.11-coreos

If your kernel is updated to at least the version corresponding to the above, some updates have been applied.

Operating systems that have **not yet released kernels with mitigation** include:

- FreeBSD 11.x
- FreeBSD 10.x

Ubuntu 17.04, which is reaching end of life on January 13, 2018 **will not receive patches**. Users are strongly encouraged to update or migrate.

**Warning:** We strongly recommend that you update or migrate off of any release that has reached end of life. These releases **do not** receive critical security updates for vulnerabilities like Meltdown and Spectre, which can put your systems and users at risk.

Because of the severity of this vulnerability, we recommend applying updates as they become available instead of waiting for a full patch set. This may require you to upgrade the kernel and reboot more than once in the coming days and weeks.

## How Do I Apply the Updates?

To update your servers, you need to update your system software once patches are available for your distribution. You can update by running your regular package manager to download the latest kernel version and then rebooting your server to switch over to the patched code.

**Note:** This article was written to be generally applicable and platform agnostic. If you are using DigitalOcean as your hosting provider and are running an older Droplet, you may have to perform an extra step before getting started.

DigitalOcean's legacy kernel management system used externally managed kernels that could be changed in the control panel. If your Droplet uses this system, you will need to configure it to use **internal kernel management** before continuing (newer Droplets use this system automatically). To check whether you need to update to internal kernels and to learn how to make the switch, read our [How To Update a DigitalOcean Server's Kernel](#) article.

For **Ubuntu** and **Debian** servers, you can update your system software by refreshing your local package index and then upgrading your system software:

```
$ sudo apt-get update
$ sudo apt-get dist-upgrade
```

For **CentOS** servers, you can download and install updated software by typing:

```
$ sudo yum update
```

For **Fedora** servers, use the `dnf` tool instead:

```
$ sudo dnf update
```

Regardless of the operating system, once the updates are applied, reboot your server to [install the new kernel](#). [SCROLL TO TOP](#)

```
$ sudo reboot
```

Once the server is back online, log in and check the active kernel against the list above to ensure that your kernel has been upgraded. Check for new updates frequently to ensure that you receive further patches as they become available.

## Additional Context

The Meltdown and Spectre family of vulnerabilities exploit performance-enhancing features within modern processors. A combination of processor features like speculative execution, privilege checking, out-of-order execution, and CPU caching allows read access to memory locations that should be out-of-bounds. The result is that unprivileged programs can be coerced into revealing sensitive data from their memory or accessing privileged memory from the kernel or other applications.

### How Does Meltdown Work?

The Meltdown vulnerability works by tricking a processor into reading an out-of-bounds memory location by taking advantage of flaws in a CPU optimization called speculative execution. The general idea works like this:

- A request is made for an illegal memory location.
- A second request is made to *conditionally* read a valid memory location *if* the first request contained a certain value.
- Using speculative execution, the processor completes the background work for both requests before checking that the initial request is invalid. Once the processor understands that the requests involve out-of-bounds memory, it correctly denies both requests. Though the results are not returned by the processor after the privilege checking code identifies the memory access as invalid, both of the accessed locations remain in the processor's cache.
- A new request is now made for the valid memory location. If it returns quickly, then the location was already in the CPU cache, indicating that the conditional request earlier was executed. Iterative use of these conditionals can be used to understand the value in out-of-bounds memory locations.

Meltdown represents a specific vulnerability that can be patched against.

### How Does Spectre Work?

Spectre also works by tricking a processor to misuse speculative execution to read restricted values. The disclosure notices describe **two variants** with different levels of complexity and impact.

For **variant 1** of Spectre, the processor is tricked into speculatively executing a read before a bounds check is enforced. First, the attacker encourages the processor to speculatively reach for a memory location beyond its valid boundaries. Then, like Meltdown, an additional instruction conditionally loads a legal address into cache based on the out-of-bounds value. Timing how long it takes to retrieve

afterwards reveals whether it was loaded into cache. This, in turn, can reveal the value of the out-of-bounds memory location.

**Variant 2** of Spectre is the most complicated both to exploit and mitigate against. Processors often speculatively execute instructions even when they encounter a conditional statement that cannot be evaluated yet. They do this by guessing the most likely result of the conditional using a mechanism called branch prediction.

Branch prediction uses the history of previous runs through a code path to pick a path to speculatively execute. This can be used by attackers to prime a processor to make an incorrect speculative decision. Because the branch selection history does not store absolute references to the decision, a processor can be fooled into choosing a branch in one part of the code even when trained in another. This can be exploited to reveal memory values outside of the acceptable range.

## Conclusion

Spectre and Meltdown represent serious security vulnerabilities; the full potential of their possible impact is still developing.

To protect yourself, be vigilant in updating your operating system software as patches are released by vendors and continue to monitor communications related to the Meltdown and Spectre vulnerabilities.

By: Justin Ellingwood

♡ Upvote (53)     Subscribe     Share



We just made it easier for you to deploy faster.

[TRY FREE](#)

### Related Tutorials

[How To Protect Your Linux Server Against the GHOST Vulnerability](#)

[SCROLL TO TOP](#)

How to Protect Your Server Against the Shellshock Bash Vulnerability

How to Protect Your Server Against the Heartbleed OpenSSL Vulnerability

How to Install TrueCrypt (CLI) on Linux

How To Use WPScan to Test for Vulnerable Plugins and Themes in Wordpress

## 68 Comments

Leave a comment...

Log In to Comment

^ [lkoenigsberger](#) January 10, 2018



1 Hi all,

for all Ubuntu 16.04 users please be aware that the kernel 4.4.0-108 is buggy!!

<https://bugs.launchpad.net/ubuntu/+source/linux/+bug/1742323>

Be sure to upgrade to kernel kernel 4.4.0-109 which was also released.

[@jellingwood](#) maybe you should update that in the post.

^ [jellingwood](#) MOD January 10, 2018



o [@lkoenigsberger](#) Thanks for the heads up. I've changed the kernel version for 16.04 to avoid the buggy release.

^ [orchetect](#) January 26, 2018



o Just did the update on Ubuntu 16.04.3, noticed the kernel is 4.4.0-112 after reboot.

^ [jamiec5692cda7931d80e27444](#) January 15, 2018



o Even after doing this on a CentOS 7.4 Droplet, spectre-meltdown-checker reports:

SCROLL TO TOP

- Mitigation 2
- Kernel compiled with retpoline option: NO
- Kernel compiled with a retpoline-aware compiler: NO > STATUS: VULNERABLE (IBRS hardware + kernel support OR kernel with retpoline are needed to mitigate the vulnerability)

How do we fix this?

---

^ [jamiec5692cda7931d80e27444](#) January 15, 2018

o Found this, which answers my question (it's a work in progress)

<https://blog.digitalocean.com/a-message-about-intel-security-findings/>

---

^ [brianjking](#) January 26, 2018

1 What is the spectre-meltdown-checker? Link? Thanks!

Edit: looks like it's probably this? <https://github.com/speed47/spectre-meltdown-checker>

---

^ [jamiec5692cda7931d80e27444](#) January 30, 2018

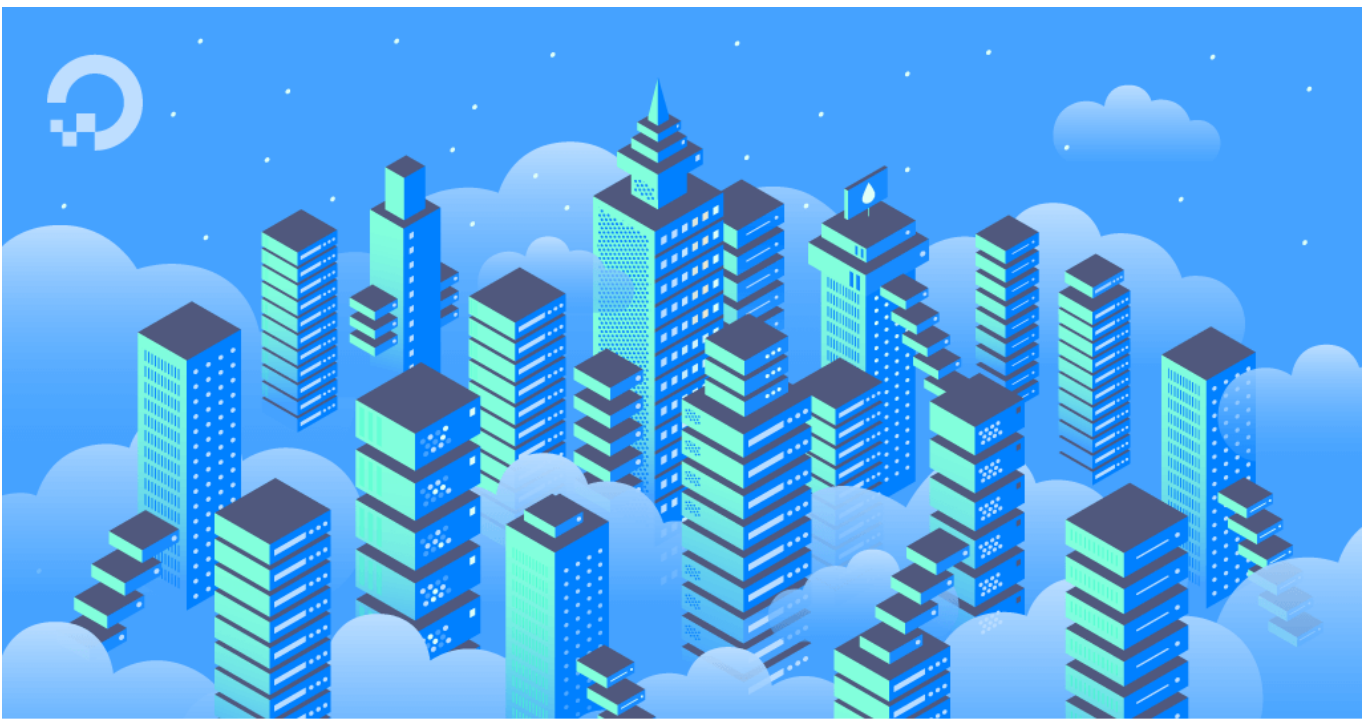
o <https://github.com/speed47/spectre-meltdown-checker>

---

^ [fgergo](#) January 16, 2018

3 If your droplet won't switch to the latest kernel after the described updates and your droplet uses "external kernel management" (ie. changing the kernel via the control panel), you might want to consider changing to "Internal Kernel Management" following <https://www.digitalocean.com/community/tutorials/how-to-update-a-digitalocean-server-s-kernel>

After that you'll be able to explicitly change to the kernel you want to use.



## How To Update a DigitalOcean Server's Kernel

by Adam LaGreca

Updating the kernel on your DigitalOcean Droplet is a straight forward process that differs slightly based on the Droplet's operating system. In this guide, we'll walk you through the process of updating your kernels for DigitalOcean Droplets.

---

^ [theluggage](#) January 27, 2018

o ty this helped me update the kernel to latest in my droplet.

---

^ [dota2shopthai](#) January 27, 2018

o thank you so much!!

---

^ [ontheocean](#) January 26, 2018

o Ubuntu 16.04 kernel is updated again, or at least before a link to this post was emailed to me today, I had just completed an upgrade to 4.4.0-112

---

^ [noITskillsatALL](#) January 26, 2018

o i have no clue what to do... for someone who is not IT at all - this is mind blowing.

---

^ [brianjking](#) January 26, 2018

1 Hopefully you have someone that is able to help you out that is managing your Droplet(s) then. Otherwise, I highly suggest moving to a managed server option from another company.

SCROLL TO TOP



---

^  nolTskillsatALL January 26, 2018

- o I don't have anyone. I am the owner of the site and everything i do on this server i have to pay and pay someone to help me. THought it would be better and easier but it seems like a never ending process - and i can't really enjoy the site because i'm worried about these new announcements and its become costly. Someone like me with no IT skills - so why not support them too.

---

^  brianjking January 26, 2018

- o If you need someone to help manage your droplet(s) contact me on Twitter at [@brianjking](https://twitter.com/brianjking) or you can find my email at <https://brianjking.io>.

---

^  lovedroppingseeds January 29, 2018

- o Thx for offering, am reaching out to ya

---

^  cryptoonia January 27, 2018

- 1 don't panic ! pirates that want to exploit meltdown or spectre are not going to target small vps & small websites even if they do if your site don't keep records of anything valuable, secret, to steal there is nothing they can steal right ?

DO have to be reactive on this (crazy imo) meltdown/spectre revelation obviously as server admin of big website with large customer database have to too, even if that means applying every single security updates as soon as they are released for them (pain in the ass clearly).

This being said if your site does keep records of valuable information, you're being careless & somewhat presumptuous not having anybody close & reachable anytime responsible for maintaining your vps. shit always happen sooner or later.

---

^  abaqueiro2 January 27, 2018

- o For the hack (vulnerability) to be exploited the attacker needs to first gain access to your droplet, and then try to read protected memory and if the attacker gets lucky find some secret in the read data, so if you are the only user (linux account) in your droplet you don't have anything to worry about.

In conclusion, do anything, the problem is for the DO team, they need to patch their Virtualizers.

By users of your system I am talking about linux accounts, like root and the others that are in /etc/passwd.

---


^  solidpixel January 27, 2018

- 1 For someone who is not IT at all, I suggest you avoid using a VPS next time, and go for a managed hosting instead :)

^  [notSkillsatALL](#) January 28, 2018

- o im stuck - cause i don't even know how to do that. (go for a managed hosting instead :)) i got on here by a friend who knows IT and he is no longer around. My buddy said this would be amazing. I guess not for someone who has no clue what a Kernel is or the black screen that you all log in to.

---

^  [lovedroppingseeds](#) January 29, 2018

- o Don't feel bad, I'm in the same boat. I thought I could have the time to figure how to use it but its over my head and the programmer is MIA.

---

^  [IMsupporting](#) January 26, 2018

- o Yum update seems to "remove" the old kernel and installs the new one on Centos 7

yet a uname -r shows the old one still.

a yum update shows no new packages waiting.

No idea what went wrong here.

---

^  [IMsupporting](#) January 26, 2018

- o Found the problem..

My droplet was using the older method where DO manage the kernel.  
I set my kernel to Grub Centos V2 and powered the VM off. ( Not a reboot)  
I then powered it on and it snow using the installed one fine.

My Centos 7 VM now shows the following after a uname -ir command.

3.10.0-693.17.1.el7.x8664 x8664

All good (so far)

---

^  [stuart701397](#) January 26, 2018

- o Just to be clear. Is simply changing the Kernel from the admin console good enough? Or do we still have to update the droplet after changing the kernel? Also some of my droplets have internally managed Kernels. What does that mean exactly?

---

^  [emotilla](#) January 26, 2018

- o \$ sudo apt-get dist-upgrade >>> is failing on Ubuntu 16.04, I get this error:

Err:1 [http://download.owncloud.org/download/repositories/stable/Ubuntu\\_16.04](http://download.owncloud.org/download/repositories/stable/Ubuntu_16.04) owncloud-files 10.0.5-1.1

404 Not Found [IP: 138.201.139.178 80]

let us know when we can try again, thanks!

---

^ mnewton January 27, 2018

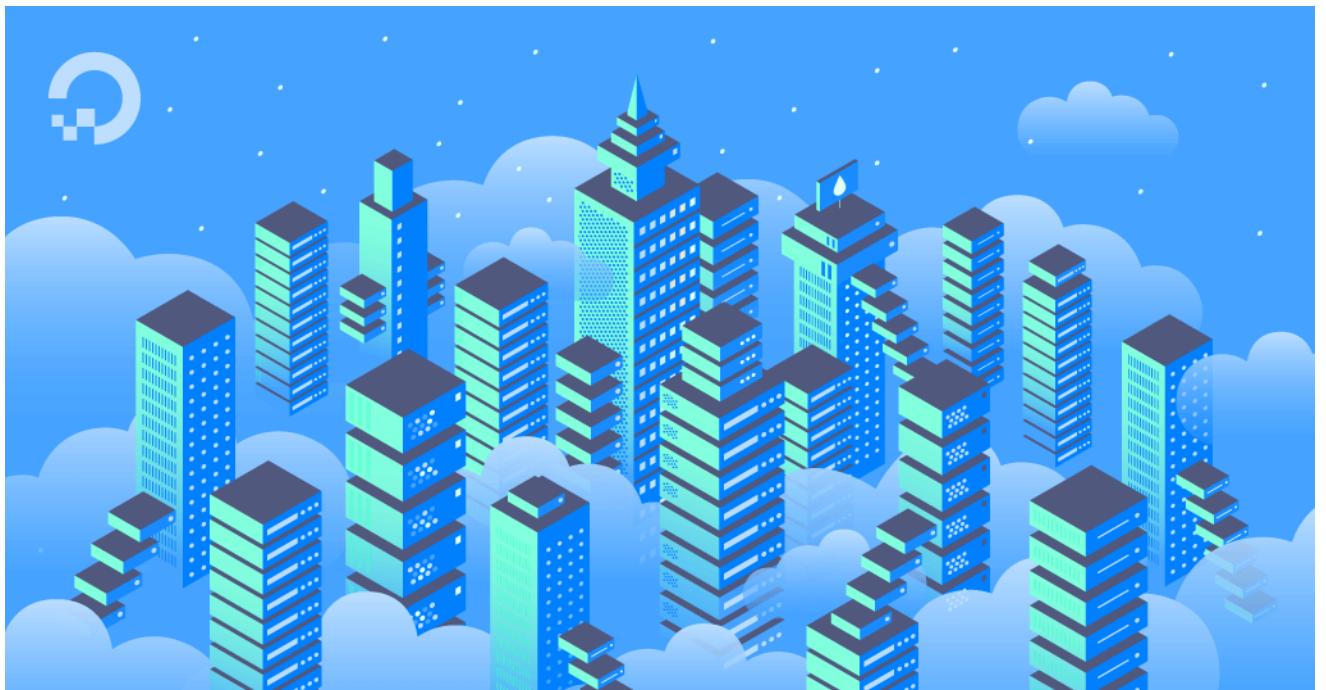
- o I'm having a bit of a tough time upgrading my kernels. Running CentOS 6, these are pretty old droplets so had to be changed to the GrubLoader kernel in the control panel. After doing that, they boot to a newer kernel, which is great. But it's not the newest kernel.

If I try running `yum upgrade kernel` it seems to work, but throws out **grubby fatal error: unable to find a suitable template** and doesn't have a new kernel on reboot. The grub conf file doesn't even reference the kernel that I *am* running, so it's clearly being ignored. Any suggestions? Any hints on how CentOS is actually deciding what kernel to run?

---

^ theluggage January 27, 2018

- o if your droplet is old, you can read this article to see how you can update your kernel management <https://www.digitalocean.com/community/tutorials/how-to-update-a-digitalocean-server-s-kernel>



### How To Update a DigitalOcean Server's Kernel

by Adam LaGrecia

Updating the kernel on your DigitalOcean Droplet is a straight forward process that differs slightly based on the Droplet's operating system. In this guide, we'll walk you through the process of updating your kernels for DigitalOcean Droplets.

---

^ mnewton January 27, 2018

- o As I said, "Running CentOS 6, these are pretty old droplets so had to be changed to the GrubLoader kernel in the control panel." Which is what that page tells you how to do. What I need to know is what bootloader DO's CentOS 6 droplets are using, and how to configure it.

---

^ hungryswede January 27, 2018

SCROLL TO TOP

<sup>1</sup> [@mnewton](#) , [@rbb3b7484510f6e5cdb0956c54](#)

I had the same issue, figured out that I needed to change to the grubloader kernel, at which point it started booting 2.6.32-696.13.2.el6.x86\_64. Although that kernel version was installed, it was not referenced by boot.conf, so I don't know why it was picked.

I tried manually making an entry for the latest kernel, 2.6.32-696.20.1.el6.x86\_64, but it still would not boot.

In the end, I got grubby to create an entry for me, having first set up a dummy entry like this in /boot/grub/grub.conf, which grubby used as a template:

```
title CentOS (2.6.32-696.13.2)
root (hd0,0)
kernel /boot/vmlinuz-2.6.32-696.13.2.el6.x8664 ro root=/dev/vda1
initrd /boot/initramfs-2.6.32-696.13.2.el6.x8664.img
```

With that entry in place, I uninstalled and reinstalled the latest kernel:

```
sudo yum erase -y kernel-2.6.32-696.20.1.el6
sudo yum install -y kernel-2.6.32-696.20.1.el6
```

And now it happy boots the correct kernel.


FWIW, the entry that grubby created, and which does work, is:

```
title CentOS (2.6.32-696.20.1.el6.x8664)
# This config for 2.6.32-696.20.1.el6.x8664 works. This kernel version is supposed to mitigate
against meltdown and spectre
root (hd0,0)
kernel /boot/vmlinuz-2.6.32-696.20.1.el6.x8664 ro root=LABEL=DOROOT crashkernel=auto
SYSFONT=latarcyrheb-sun16 LANG=enUS.UTF-8 KEYTABLE=us
initrd /boot/initramfs-2.6.32-696.20.1.el6.x86_64.img
```

It would be nice if this page, as well as the other articles about changing kernels, would mention that you have to manually set up the correct entry in grub.conf. I'm guessing that grubby didn't like something about the older entries created by DO, as I can't recall ever having to manually add entries - normally, that's handled when you install a new kernel via yum/rpm.

---

 [mnewton](#) January 30, 2018

-  Yeah it seems like grub.conf isn't even read, as mine had only 2.6.32-431 in it, but was running 2.6.32-696.1. But at least fixing the file got rid of the grubby error, and now the file updates with yum.

---

 [rbb3b7484510f6e5cdb0956c54](#) January 27, 2018

- <sup>1</sup> I had similar issue with centos-6.6. An article says to 'rpm -e' the older kernel versions. After doing that my kernel still failed to change. But /boot/ dir had complete sets of files from both the old and new kernel.

By moving those old /boot/ kernel files away also (not just 'rpm -e'), my droplet did change kernels finally (2.6.32-696.20.1.el6.x86\_64). I guess you really have to commit to it.

 [mnewton](#) January 30, 2018

0 Yeah that was the final step, thanks.

---

 [Ryukk](#) January 27, 2018

0 I don't want to UPGRADE my whole OS

Just give required update please

---

 [Ryukk](#) January 27, 2018

0 And please TIME to offer AMD CPUs, enough of this Intel crap

---

 [cayxxx](#) January 27, 2018

0 I'm confused about my situation. My host is running on CentOS 6.9 provided by you. But I've changed the kernel from 2.6.32-696.18.7.el6.x8664 to 4.14.14-1.el6.elrepo.x8664 recently. What should I do ?

---

 [demoskp](#) January 27, 2018

1 I have Ubuntu 16.04 and when running the upgrade I am getting the following message:

"A new version of /boot/grub/menu.lst is available, but the version installed currently has been locally modified.

What would you like to do about menu.lst?"

When I select the option "show side-byside difference between the versions" I get the following:

Line by line differences between versions

```
|
| Old file: /run/grub/menu.lst root.root 0644 2018-01-27 12
| New file: /tmp/fileCrfBIN root.root 0600 2018-01-27 12:08
|
| ## ## End Default Options ## ## ## End Default Options ##
|
| title Ubuntu 16.04.3 LTS, kernel 4.4.0-97-generic title U
| root (hd0) root (hd0)
| kernel /boot/vmlinuz-4.4.0-97-generic root=LABEL=clo kern
| initrd /boot/initrd.img-4.4.0-97-generic initrd /boot/ini
|
| title Ubuntu 16.04.3 LTS, kernel 4.4.0-97-generic ( title
| root (hd0) root (hd0)
| kernel /boot/vmlinuz-4.4.0-97-generic root=LABEL=clo kern
| initrd /boot/initrd.img-4.4.0-97-generic initrd /boot/ini
|
| ### END DEBIAN AUTOMAGIC KERNELS LIST # SCROLL TO TOP
```

What do I select now?

---

^ [AlexWebcicles](#) February 2, 2018

- o That one actually has no difference other than whitespace if you select to show just the differences. You will get another prompt with differences, though, where I opted to keep the existing version. I believe DO uses grub and are the ones who set up the menu.list, it's something AWS does I know, and you might break something by switching it back to default. I don't know for sure the dirty details, but everything is working properly with it on my servers.

---

^ [kacnje](#) January 27, 2018

- o I have Droplet with Ubuntu server 17.10.  
Here I can read that patched version is "kernel 4.13.0-25-generic".  
I have updated server with "apt-get update", "apt-get upgrade", "apt-get install linux-image-generic" and everything is finished fine.

But, when I check with "uname -a", I get information the "4.13.0-19-generic" is used.  
How can I upgrade to latest kernel?

---

^ [kacnje](#) January 28, 2018

- o Solved. After second restart it shows "kernel 4.13.0-32-generic".

---

^ [vincentblouin](#) January 27, 2018

- o For Ubuntu 16.04 is "dist-upgrade" necessary ? I simply did "upgrade" instead and rebooted and my kernel version is  
"4.4.0-112-generic"  
which is higher than the recommended  
"4.4.0-109-generic"  
Isn't a simple "upgrade" sufficient and less risky than a "dist-upgrade" ?

---

^ [mranderson](#) January 27, 2018

- o I'm currently running: **Ubuntu 14.04.5 LTS (GNU/Linux 3.13.0-57-generic x86\_64)**

I ran the update commands:

```
sudo apt-get update && sudo apt-get dist-upgrade
```

I saw this show up at the end of the dist-upgrade:

```
update-initramfs: Generating /boot/initrd.img-3.13.0-141-generic
```

SCROLL TO TOP

but after I restarted, I'm still seeming my old kernel version in the welcome message and when running `uname -a` ...

Am I doing something wrong here?

---

 [dobomkft](#) January 28, 2018

o Same here!

A was running:

**14.04.5 (GNU/Linux 3.13.0-57-generic x86\_64)**

I even upgraded my release, and now am running:

**16.04.3 LTS (GNU/Linux 3.13.0-57-generic x86\_64)**

I've ran

**sudo grub-update**

then

**sudo reboot**

but it made no difference even though my kernel image list already includes 4.4.0-112-generic

I tried modifying my `etc/default/grub` file so the **DEFAULT=1** instead of 0, but that didn't help either.

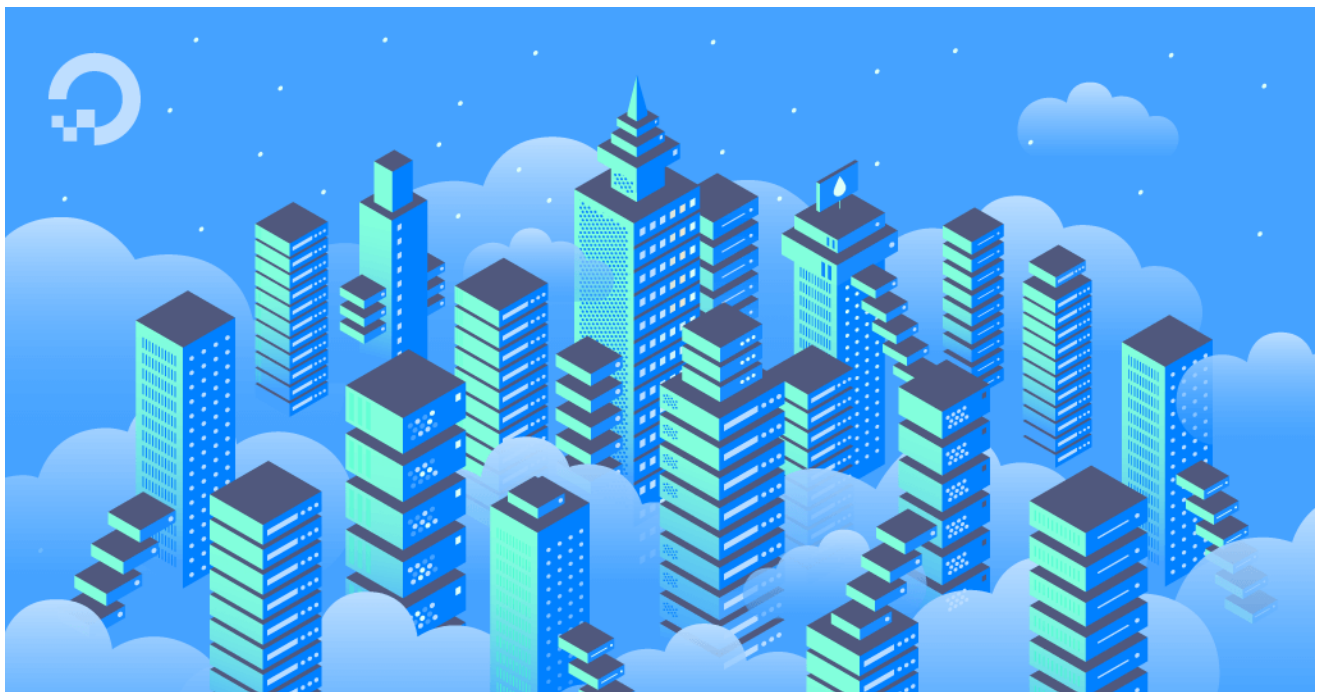
The article mentioned above looks very promising:

<https://www.digitalocean.com/community/tutorials/how-to-update-a-digitalocean-server-s-kernel>

It turns out that my droplet is using "legacy external kernel management", because I see a dropdown on my digitalocean Settings/Kernel page.

1. I first selected GrubLoader v0.2, but I was unable to connect to the server.
2. I then selected GrubLoader v0.1, and I finally reached the GrubLoader itself by opening the console from the digitalocean admin,
3. I selected Advanced Ubuntu form the list,
4. and there was a list of the kernels I installed earlier.
5. I selected 4.4.0-112-generic
6. Had to wait about 4 minutes until it loaded
7. I reopened my SSH connection and WOW
8. I'm now running 4.4.0-112-generic!





## How To Update a DigitalOcean Server's Kernel

by Adam LaGreca

Updating the kernel on your DigitalOcean Droplet is a straight forward process that differs slightly based on the Droplet's operating system. In this guide, we'll walk you through the process of updating your kernels for DigitalOcean Droplets.

^ erelsgl January 28, 2018



0

I have Ubuntu 14.04 and I do not want to update to 16.04 using "dist-upgrade" since this will cause some of my programs to stop working.

How can I update the kernel of 14.04 without upgrading to 16.04?

^ dobomkft January 29, 2018



2 dist-upgrade doesn't upgrade to a new release, that's do-release-upgrade.

*(I see my comment may have been misleading, I should have left out the release upgrade part!)*

There's an explanation here:

<https://askubuntu.com/a/215276>

So it depends on how you have kernel management setup with your droplet in the digitalocean admin. if it's set to internal, then all you have to do is:

- *Create a snapshot of your droplet in case things don't work as expected!*
- `sudo apt-get update`
- `sudo apt-get dist-upgrade`
- `sudo reboot`

If there is no change in the kernel version then, you probably have external kernel mar  
Then you must:

SCROLL TO TOP




- in digitalocean admin droplet/settings/kernel
- select grub v1 or v2 from dropdown
- ssh: `sudo poweroff`
- digitalocean admin droplet switch on, wait until it turns on.
- log in with ssh (if you can't log in, then try the other grub version, power off again and on)
- check kernel version

That's it!

Worked for me, hope it works for you too.

---

 [pablotomasruiz](#) January 29, 2018

1 Working!  
Thanks.

---

 [ivanrlio](#) January 30, 2018

0 Hey.

I'm on 14.04 Trusty, and I've followed the instructions as per the article, however, I'm still currently running **4.4.0-53-generic**. Kernal management is internal (<https://snag.gy/PalKzv.jpg>) so I'm not too sure why it isn't working even after a `sudo reboot`.

Any ideas?

Thanks!

---

 [dobomkft](#) January 31, 2018

0 You can check what kernel images are installed by:

```
dpkg --get-architecture | grep linux-image
```

If there is a newer version in the list then the question is why grub doesn't select the newest kernel on reboot.

---

 [ivanrlio](#) February 1, 2018

0 Hey,

Thanks for your reply. I get a long list, but this is the very last one,

```
for version 3.13.0 on 64 bit x86 SMP
```

```
ii linux-image-generic
```

```
3.13.0.141.151
```

SCROLL TO TOP

Thanks

---

^ [dobomkft](#) February 1, 2018



0 Hi!

For some reason I can't reply to your second message, so I'll reply here.

So according to that, the new image is present, then the question is why grub doesn't boot off of it. Since I had external kernel management, and solved my problem the mentioned way, I'm not sure what will solve your situation, but I would probably try:

- `sudo update-grub`
- `sudo reboot`

If that doesn't help, then you may have to edit grub config file...

You might find something helpful here:

<https://superuser.com/questions/208502/how-to-add-a-new-kernel-to-grub2>

Good luck!

---

^ [alcampagnani](#) February 5, 2018



0 After that, HTTPS 2.0 stopped working on apache.

Someone knows why and what can i do!??

---

^ [TuomasL](#) March 7, 2018



1 Thanks. This worked for me.

So my 14.04 Droplet got the latest kernel with these steps:

1. Snapshot just in case...
2. `sudo apt-get update`
3. `sudo apt-get dist-upgrade`
4. `sudo reboot`
5. Digitalocean admin droplet > settings > kernel
6. Selected "DigitalOcean GrubLoader v0.1 (20160527)" (someone mentioned v0.2 wouldn't connect for them, so didn't even try)
7. `sudo poweroff`
8. Digitalocean admin droplet on

Logged back in and I see kernel 3.13.0-142, which I believe is the latest.  
Thanks again for the tip.

---

^ [adam3ed4093c50b](#) January 28, 2018

1 If it helps, I've just run through this process with lots of CentOS 6 boxes.

The yum update kernel\* worked great, but had to do two things to get the instance to pick up the new kernel  
1 - in the DO control panel, under Kernel, select their GRUB loader version 0.2  
2 - rpm -q kernel lists all the kernels installed. I used rpm -e to remove all the older versions - and the instance then booted into the latest kernel

Hope this helps - this is a brief summary of quite a few hours work updating tons of boxes!

---

^ [Scopp](#) January 28, 2018

0 I did follow the steps, rebooted the system and everything, but looks like my kernel version hasn't been updated.

```
~$ sudo apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
libc-ares2 libv8-3.14.5 linux-headers-3.13.0-68
linux-headers-3.13.0-68-generic linux-image-3.13.0-68-generic
linux-image-extra-3.13.0-68-generic
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

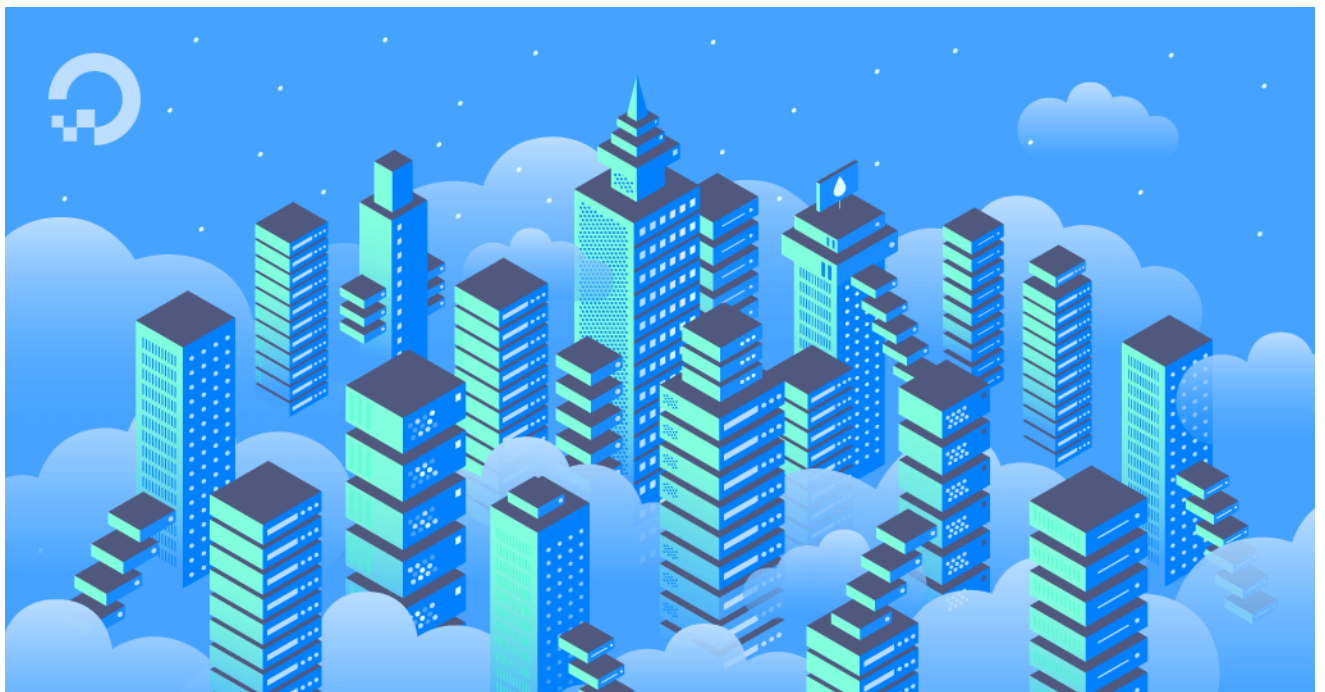
```
~$ hostnamectl status
Static hostname: dc-01
Icon name: computer-vm
Chassis: vm
Boot ID: 6658869fb9574f3186f8201ab51d44b8
Operating System: Ubuntu 14.04.5 LTS
Kernel: Linux 3.13.0-57-generic
Architecture: x86_64
```

---

^ [dobomkft](#) January 30, 2018

0 Have you tried what I suggested here?

<https://www.digitalocean.com/community/tutorials/how-to-protect-your-server-against-the-meltdown-and-spectre-vulnerabilities?comment=67549>



## How To Protect Your Server Against the Meltdown and Spectre Vulnerabilities

by Justin Ellingwood

On January 4, 2018, multiple vulnerabilities with the design of modern CPUs were disclosed. Taking advantage of certain processor performance optimizations, these vulnerabilities, named Meltdown and Spectre, make it possible for attackers to coerce...

^ [Scopp](#) January 30, 2018



1 Looks like it worked.

Droplet was using grub loader v0.2, so I changed it to v0.1.

Then I changed it back to v0.2 (I guess the newer version the better, right?) and the kernel version is now Linux 3.13.0-141-generic.

Thanks :)

Load More Comments



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.



Copyright © 2019 DigitalOcean™ Inc.

[Community](#) [Tutorials](#) [Questions](#) [Projects](#) [Tags](#) [Newsletter](#) [RSS](#) 

---

[Distros & One-Click Apps](#) [Terms, Privacy, & Copyright](#) [Security](#) [Report a Bug](#) [Write for DOnations](#) [Shop](#)