**CentOS patching – 8 best practices to follow**

Maintaining a server can be really hard.

Applying regular updates and patches is important to keep the Operating system up to date and secure.

In our [Server Management Services](https://bobcares.com/outsourced-server-support-services/), we help server owners forget their server concerns by keeping the servers secure, update the server software and install critical patches on time.

Today, let’s discuss more on “***CentOS patching – best practices***“.

What is a Patch and Why to Patch?

Patches are updates that contain changes in source code and are installed into the existing software program.

Here’s what patches can do:

* Address new security vulnerabilities.
* Integrate new features.
* Address a specific bug or flaw.
* Improve Operating system/software stability.
* Install new drivers.

Why to Patch?

Unpatched systems are one of the easiest entry points for hackers to gain access to the network.

So, patches to an Operating system are essential to keep the systems up to date, stable and safe from malware and other security threats.

Now, let’s see the best practices to patch a CentOS server.

CentOS Patching – Best Practices

In our experience managing servers, below are the common steps that our [Server Experts](https://bobcares.com/outsourced-server-support-services/) follow while patching CentOS servers.

1) Develop an updated inventory list

Firstly, we develop an up to date inventory of systems like OS types, OS versions, IP addresses in the system, etc.

This helps us to easily identify which patches are needed by each system.

Therefore, this keeps the patch management process up to date.

At Bobcares, for the servers that we manage, we regularly audit the servers and update the new software additions or resource additions in our inventory.

2) Schedule regular patching

Usually, CentOS releases their patches at different times.

So, our [Server Management Team](https://bobcares.com/outsourced-server-support-services/) schedule check for patches and updates atleast once a month.

Also, we regularly check for critical patches and apply them that are released in between.

In CentOS servers with EPEL repository, we use “***yum-plugin-security”*** package to install security updates.

For example, we use the below command in Centos 6/7 to list all security updates.

yum updateinfo list security all

And, we use the below command to install all security packages.

yum update --security

Unfortunately, this will not work on CentOS as it does not supply the necessary data in the yum repositories to allow the yum -plugin-security plugin to work at all. That’s why, we just run *yum update* on a regular basis to get all the security updates.

3) Schedule automatic patching

Moreover, we setup automatic patch management system to keep systems up to date with latest security patches and updates.

On CentOS servers, we use the package “***yum-cron***” to automate the security updates via yum.

First, we install this package with the command:

yum -y install yum-cron

After the installation is complete, we start the service, and enable it to automatically start on server boot with the below commands:

systemctl start yum-cron

systemctl enable yum-cron

Finally, we modify the file “***/etc/yum/yum-cron.conf***” for automatic updates.

For example, to automatically install security updates, we modify the below parameter in the *yum-cron.conf* file.

update\_cmd = security

4) Download patches from trusted source

This is one of the most important steps in Centos patching.

When updating software, it is important to download the updates or patches from a trusted source.

Because, an attacker can easily rebuild and release a package as the one that is supposed to fix the problem but with a different security exploit.

At Bobcares, Our [Security Engineers](https://bobcares.com/outsourced-server-support-services/), always download RPMs from trusted sources and verify the package for its integrity.

For example, in Centos all packages are signed with *GPG* *key* that guarantees the authenticity of the files.

5) Prioritize the patches based on severity

Some patches must be applied immediately to prevent malicious access to your network.

Likewise, some may have only a minimal effect on certain system configurations.

So, we first assess the level of vulnerability, severity and the cost of mitigating each attack and then prioritize the patches like Critical, Urgent, etc.

6) Test the patches

Server patches can conflict with your systems and take down the system completely.

In other words, patches require certain system requirements for installation, and if they are not properly tested, the dependent systems or applications may go down.

So, before applying the patches, it’s always recommended to test the patches on a test environment.

During this phase, we identify whether the server requires a reboot. If so, our [Server Management Team](https://bobcares.com/outsourced-server-support-services/) plans a maintenance window to apply these patches in the live system.

7) Schedule a Downtime or maintenance window

Patching requires time, reboots, that can interrupt normal business operations.

That’s why, we often maintain a scheduled maintenance window for such activities.

So, customers can plan their business activities accordingly. Also, there are no unexpected reboots that disrupt business operations.

At Bobcares, our [System Engineers](https://bobcares.com/outsourced-server-support-services/), often schedule such patches/updates during weekends at off peak hours so customers have minimal impact.

8) Have a good backup

Above all, we always take a complete backup of the system before applying the patch.

So that, if something goes wrong, we can easily roll back to the previous version.

Conclusion

Patches are important to make the system secure and stable. With a little planning ahead, patching can be a smooth process. Today, we discussed more about  ***CentOSpatching best practices*** and the steps our [Server Administration Team](https://bobcares.com/outsourced-server-support-services/) took to make it a pain free process.