

Forum:[Hack Forums](#)

Thread: [Question Related to Pornhub Bug](#)

Nick Jones - April 6, 2017, 9:54 pm

I was reading a blog on pornhub bug and i got question on my mind

This is blog

[https \[.\] //blog\[.\]zsec.uk/pwning-pornhub](https://blog[.]zsec.uk/pwning-pornhub)

There he wrote this

[https \[.\] //pastebin\[.\]com/Nvvj1F6M](https://pastebin[.]com/Nvvj1F6M)

So i want to know what malicious thing can attacker do with that nc and how ?

I need practical example

Mr. Robot - April 6, 2017, 9:55 pm

And I quote

Quote:Further investigation uncovered that there are more malicious commands that can be run, including clearing the system or causing an overflow.

This issue has now been fixed, pornhub have closed the port and removed the service

Look at the memcached service for different commands

<https://github.com/memcached/memcached/wiki>

Nick Jones - April 6, 2017, 10:03 pm

Some of the popular Web Applications like YouTube, Wikipedia, and Twitter are using Memcache for performance boosting.

Ref: [http \[.\] //memcached.org/](http://memcached.org/)

So if pornhub removing this "memcache service" because of malicious things then why such Youtube,Wikipedia using such service yet ?

Still exploring it with googling and i read this

Quote:What is its importance in a Penetration Test?

Ideally, this service should be running in a protected environment behind firewalls; accessible only to the web server. If exposed over the internet then it can enable a pentester to add, update and delete the data being cached in the Memcache.

So why pornhub remove service instead using this service behind firewall ?Can that firewall also be hack ?

pop.pop.ret - April 7, 2017, 6:28 am

(Apr 6, 2017 10:03 PM)Nick Jones Wrote: [\[CITE\]](#) Some of the popular Web Applications like YouTube, Wikipedia, and Twitter are using Memcache for performance boosting.

Ref: [http \[.\] //memcached.org/](http://memcached.org/)

So if pornhub removing this "memcache service" because of malicious things then why such Youtube,Wikipedia using such service yet ?

Still exploring it with googling and i read this

So why pornhub remove service instead using this service behind firewall ?Can that firewall also be hack ?

because its not memcached itself that is the issue. That's like saying you should disallow file:// uri scheme because it can be exploited as a result of an SSRF vuln file.