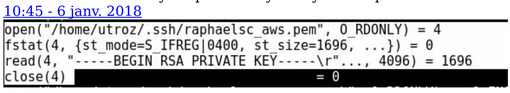
Raphael Carvalho
@raphael_scarv

just found out that #SSH doesn't use DIRECT IO to open *.pem, which means private key goes to page cache, which means attacker may exploit meltdown to discover your private key. I may come up with a POC. Watch it! #MELTDOWN pic.twitter.com/1NuYzFWGBd
10:45 - 6 janv. 2018



Twitter
par: Raphael Carvalho @raphael_scarv

Cliff O'Sullivan 6 janv.
@cliffsull
En réponse à @raphael_scarv
Thanks for sharing
Afficher la conversation ·

Raphael Carvalho 6 janv.
@raphael_scarv
En réponse à @raphael_scarv
BTW, I'm basing my work on a tool I created which exploits #meltdown to determine whether or not host is affected by the vulnerability, follow it: github.com/raphaelsc/Am-I...
Afficher la conversation ·

Péricles L. Machado 6 janv.
@_pmachado_
En réponse à @raphael_scarv
Did you try violate the virtual machine encapsulation? Or try to access the host machine from a LXC or docker?
Afficher la conversation ·

Raphael Carvalho 6 janv.
@raphael_scarv
En réponse à @_pmachado_
Pericles, not yet, but reading the papers and docs out there, I have seen security researchers saying they can inspect data of other guests in a shared tenant environment in the cloud
Afficher la conversation ·

Dick Morrell 6 janv.
@TheSecurityBod
En réponse à @raphael_scarv @_pmachado_
Raphael keep up the good work
Afficher la conversation ·

Raphael Carvalho 6 janv.
@raphael_scarv
En réponse à @TheSecurityBod @_pmachado_
thanks, Dick!
Afficher la conversation ·

Crypto Pietje [NO176] 7 janv.
@CryptoPietje
En réponse à @raphael_scarv
Is this true for all SSH implementations or 'just' a specific one like OpenSSL?
Afficher la conversation ·

locotx_ftw_2002 7 janv.
@locotx_ftw_2002
En réponse à @raphael_scarv
Interesting.
Afficher la conversation ·

Evan Klitzke 7 janv.
@eklitzke
En réponse à @raphael_scarv
Really unfortunate that we live in a world where O_DIRECT can be considered a security measure.
Afficher la conversation ·

Raphael Carvalho 7 janv.
@raphael_scarv
En réponse à @CryptoPietje @CryptoYoda1338
@CryptoYoda1338 not sure about other implementations, but this one is pretty much used everywhere. We all trusted Intel when writing our software for proper isolation, and when that is broken, we're basically all doomed. We should patch our systems AS FAST AS POSSIBLE!
Afficher la conversation ·

Joseph LeRoy 7 janv.
@josephbleroy
En réponse à @raphael_scarv
So from my understanding, anyone who shares the same physical system on a cloud provider (such as AWS) has the ability to read my SSH private key contents from memory?
Afficher la conversation ·

Joseph LeRoy 7 janv.
@josephbleroy
En réponse à @raphael_scarv
In theory, they would be able to gain access to my system if they retrieved my private key. Ways to mitigate this would be to whitelist only certain IP addresses from logging in locally / remotely and setting up MFA. Does this sound correct?
Afficher la conversation ·

Martin Sundhaug 7 janv.
@sundhaug92
En réponse à @raphael_scarv @CryptoPietje @CryptoYoda1338
tbf, it's a bit hard to not trust your CPU
Afficher la conversation ·

Martin Sundhaug 7 janv.
@sundhaug92
En réponse à @raphael_scarv @CryptoPietje @CryptoYoda1338
It's like not trusting physics
Afficher la conversation ·

Raphael Carvalho 7 janv.
@raphael_scarv
En réponse à @raphael_scarv
For anyone interested, direct io (cache bypassing) would only tighten the time range the private key is vulnerable. In other words, private key would be vulnerable while ssh program is running, whereas right now private key is vulnerable while it is not purged from page cache.
Afficher la conversation ·

Raphael Carvalho 7 janv.
@raphael_scarv
En réponse à @josephbleroy
Don't know yet to which extent malicious guest sharing host could get into host's address space, but assuming it can read all kernel space, it has access to all RAM which is mapped in the kernel space, meaning your private key is vulnerable :-(
Afficher la conversation ·

dnet 7 janv.
@dn3t
En réponse à @leyrer @raphael_scarv
when you have your private keys in *.pem files instead of dedicated HW (smart card, HSM), you have deeper issues
Afficher la conversation ·

Gunstick 7 janv.
@GunstickULM
En réponse à @raphael_scarv @Ministraitor
While you are at it, how vulerable are keys in ssh-agent?
Afficher la conversation ·