Заштита на neoCloud од L1TF

04/24/2024 15:41:33

FAQ Article Print

Category:	General	**Votes:**	0
State:	public (all)	**Result:**	0.00 %
Language:	mk	**Last update:**	14:38:33 - 12/12/2018

Keywords

Security L1TF

Symptom (public)

Problem (public)

Layer 1 Terminal Fault е безбедносен пропуст во Intel процесорите кој овозможува неовластено преземање на информации и податоци од Layer 1 Cache. Од овој проблем најмногу се афкетирани виртуелните околина бидејќи преземањето може да се изврши од страна на виртуелни машини кои работат на исто hyper-threading јадро на процесорот. Пропустите се врз база на претходно објавените Speculative-Execution vulnerabilities. Повеќе информации на следниот линк и на ликовите во Solution секцијата.

[1]https://www.intel.com/content/www/us/en/architecture-and-technology/l1tf.html

[1] https://www.intel.com/content/www/us/en/architecture-and-technology/l1tf.html

Solution (public)

Заштита на инфраструктурата на neoCloud Серизониот импакт на пропустите кај виртуелните околини, на што е базирана секоја Cloud околина и каде се хостирани податоци на различни корисници, нè принуди да ги имплементираме безбедносните закрпи за L1TF во најкраток можен рок. За заштита на инфраструктурата на neoCloud, потребно е да се надградат и ажурираат следните компоненти: Надградба на System ROM Согласно препораките од HPE, System ROM на серверите потребно е да се надгради на верзија понова од 2018.05.21 Надградба на vSphere виртуелната околина Согласно безбедносните препораки од VMware искажани во VMSA-2018-0020, за vSphere 6.5, која е инсталирана на инфраструктурата на neoCloud, потребно е да се надгради vCenter Server на верзија 6.5u2c додека ESXi да се надгради со следните закрпи:
- ESXi650-201808401-BG
- ESXi650-201808402-BG
- ESXi650-201808403-BG

Со самата инсталација на закрпите, се овозможува заштита од Sequential-context attack vector. Дополнително, во ESXi оперативниот систем на серверот е овозможена напредната опција VMkernel.Boot.hyperthreadingMitigation со што се овозможува заштита од Concurrent-context attack vector. Надградба на оперативните системи Бидејќи со самата надградба на серверите и на виртуелната околина оневозможува паралелна работа на два логички процесори на едно hyperthreading јадро, оперативниот систем од една виртуелна машина неможе да пристапи до L1 Chache на друга виртуелна машина или на самиот хост. Затоа, надградбите на оперативните системи ќе се извршуваат во рамките на редовните 3 месечни надградби. Заштита на клиентски виртуелни машини Бидејќи со самата надградба на серверите и на виртуелната околина оневозможува паралелна работа на два логички процесори на едно hyperthreading јадро, оперативниот систем од една виртуелна машина неможе да пристапи до L1 Chache на друга виртуелна машина или на самиот хост. Сепак, Microsoft и Linux заедницата препорачуваат ажурирање на виртуелните машини, со што доаѓа и нашата препорака до корисниците да ги ажурираат своите виртуелни машини во neoCloud. Преземени активности 20-23.08.2018
- Детално информирање за безбедносните пропусти, начините за напад, што е потребно за заштита и можни влијанија од заштитата
- Анализа на виртуелните околина за можно влијание на перформанси од надградба
- Припрема за надградба и детално планирање
- Надградба на System ROM на серверите во виртуелната околина за управување
- Надградба на VMware vCenter Server за виртуелната околина за управување
- Надградба на VMware vCenter Server за виртуелната околина за клиенти
- Ажурирање на VMware ESXi на серверите во виртуелната околина за управување

24-28.08.2018
- Верификација на извршените надградби
- Мониторинг на стабилност на околината
- Мониторинг за влијание на перформанси

29-31.08.2018
- Надградба на System ROM на серверите во виртуелната околина за клиент
- Ажурирање на VMware ESXi на серверите во виртуелната околина за клиенти
- Верификација на извршените надградби
- Мониторинг на стабилност на околината

Надворешни линкови HPE
[1]https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-hpesbhf03874en_us
VMware [2]https://kb.vmware.com/s/article/55636

Microsoft
[3]https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv180018

[1] https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-hpesbhf03874en_us
[2] https://kb.vmware.com/s/article/55636
[3] https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv180018