

Заштита на neoCloud од Spectre и Meltdown

04/25/2024 19:52:48

FAQ Article Print

Category:	General	Votes:	0
State:	public (all)	Result:	0.00 %
Language:	mk	Last update:	14:01:43 - 08/24/2018

Keywords

Security Spectre Meltdown

Symptom (public)

Problem (public)

Spectre и Meltdown безбедносните пропусти овозможуваат процеси неовластено да преземат информации и податоци од други процеси во рамките на еден сервер или виртуелна машина со т.н. speculative execution и indirect branch prediction. Повеќе информации на следниот линк и на ликовите во Solution секцијата.

[1] <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00088.html>

[1] <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00088.html>

Solution (public)

Заштита на инфраструктурата на neoCloud 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 2018.01.22(A) Надградба на vSphere виртуелната околина Согласно безбедносните препораки од VMware искажани во VMSA-2018-0004.3, за vSphere 6.5, која е инсталирана на инфраструктурата на neoCloud, потребно е да се надгради vCenter Server на верзија 6.5u1g додека ESXi да се ажурира со следните закрпи:
- ESXi650-201803401-BG
- ESXi650-201803402-BG

Со самата инсталација на закрпите и рестарт на серверите се активира заштитата за безбедносните пропусти. Надградба на оперативни системи Согласно препораките од Microsoft, Linux заедницата и прозиводителите на софтверски решенија потребно е да се ажурираат оперативните системи со потребните безбедносни закрпи и кај некои оперативни системи дополнително да се активираат закрпите. Заштита на клиентски виртуелни машини За заштита на клиентските виртуелни машини потребно е самите корисници да ги ажурираат и активираат безбедносните закрпи во виртуелните машини кои ги хостираат во neoCloud инфраструктурата. Преземени активности Иако безбедносните закани беа објавени во Јануари 2018, многу брзо по објавата и појавувањето на иницијалните закрпи, прозводителите HPE и VMware ги повлекоа истите заради проблеми во System ROM за Intel процесорите и во самите закрпи за хипервизорите. Од таа причина, заради зголемување на стабилноста на инфраструктурата на neoCloud, закрпите не беа применети се додека не се појавија нови верзии на System ROM и закрпи од производителите. И по самото појавување на закрпите, одлучивме дека треба да почекаме уште одреден период пред аплицирањето на истите во клиентската инфраструктура. Јануари 2018 Надградба на VMware vCenter Server за виртуелната околина за управување Надградба на VMware vCenter Server за виртуелната околина за клиенти Ажурирање на Microsoft и Linux оперативните системи во менаџмент инфраструктурата Април 2018 Истражување и припрема за инсталација на безбедносните закрпи Надградба на System ROM на серверите во виртуелната околина за управување Ажурирање на VMware ESXi во виртуелната околина за управување Активирање на заштита во Microsoft оперативните системи Јули 2018 Надградба на System ROM на серверите во виртуелната околина за клиенти Ажурирање на VMware ESXi во виртуелната околина за управување Надворешни линкови HPE

[1] https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00039267en_us
Microsoft [2] <https://support.microsoft.com/help/4072698>
VMware [3] <https://kb.vmware.com/s/article/52245>

[1] https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00039267en_us
[2] <https://support.microsoft.com/help/4072698>
[3] <https://kb.vmware.com/s/article/52245>