

# Заштита на neoCloud од MDS

04/17/2024 22:15:58

FAQ Article Print

<b>Category:</b>	General	<b>Votes:</b>	0
<b>State:</b>	public (all)	<b>Result:</b>	0.00 %
<b>Language:</b>	mk	<b>Last update:</b>	23:01:45 - 08/23/2019

## Keywords

Security MDS

## Symptom (public)

### Problem (public)

На 14.05.2019 компанијата Intel објави 4 нови напади базирани на speculative execution side channel пропустите, колективно именувани како Microarchitectural Data Sampling (MDS). Нападите овозможуваат извршување на код на систем за преземање на податоци кои треба да бидат заштитени од механизми во архитектурата на процесорот. Нападите ги опфаќаат виртуелните околии заради можноста за преземање на податоци помеѓу виртуелни машини (Inter-VM) и во рамките на виртуелна машина (Intra-VM).

Повеќе информации може да се најдат на следниот линк и на линковите дадени во Solutions секцијата.

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

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

### Solution (public)

Заштита на инфраструктурата на neoCloud Заштитата на neoCloud инфраструктурата и виртуелните машини кои се хостираат од MDS нападите, опфаќа имплементација на закрпи на следните нивоа:

- Hypervisor-Specific Mitigations - заштита на ниво на хипервизорот со цел затворање на вектори за напад помеѓу виртуелни машини и во рамките на виртуелна машина.
- Hypervisor-Assisted Guest Mitigations - заштита на ниво на хипервизор со цел затворање на вектори за напад во рамките на виртуелна машина.
- Operating System-Specific Mitigations - заштита на ниво на оперативен систем со цел затворање на вектори за напад во рамките на виртуелна машина.
- Microsoft Mitigations - заштита на ниво на процесор на сервери преку инсталација на SystemROM со цел затворање на вектори за напад.

Надградба на SystemROM на сервери Согласно препораките од HPE, System ROM на серверите потребно е да се надгради на верзија 2019.05.24(A) Надградба на vSphere виртуелна околина

Со надградба на vSphere виртуелната околина според безбедносните препораки од VMware исказани во VMSA-2019-0008 ќе се воведат Hypervisor-Specific и Hypervisor-Assisted Guest заштита. Заштитата ги опфаќа следните закрпи:

- надградба на VMware vCenter Server 6.7 на верзија U2
- инсталација на закрпи за VMware ESXi 6.5 U3
- ESXi650-201905401-BG
- ESXi650-201905402-BG2

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 Согласно препораките од Microsoft, Linux заедницата и производителите на софтверски решенија потребно е да се ажурираат оперативните системи со потребните безбедносни закрпи и кај некои оперативни системи дополнително да се активираат закрпите. Во поглед на оперативните системи во менаџмент инфраструктурата на neoCloud, истите ќе се ажурираат штом се имплементираат закрпите на ниво на хипервизор. Заштита на клиентски виртуелни машини За целосна заштита, потребно клиентите да ги ажурираат оперативните системи кои се хостираат во neoCloud со последните достапни закрпи или закрпи кои се специфични за MDS.

Дополнително, по инсталација на хипервизорските закрпи од наша страна, потребно е да се направи Power Off и Power On на виртуелните машини (рестарт не е доволен) со цел овозможување на MD\_CLEAR инструкциите, како што е опишано во [1] VMware KB 68024. Преземени активности 15.05.2019 - Креирање на иницијалниот документ, иницијално информирање за пропустите и започнување на анализа на импакт и резолуција  
06.06.2019 - Завршување на анализата, објавување на потребни закрпи и започнување на имплементација на закрпи во тестна околина  
24.06.2019 - Завршена имплементација на надградби и закрпи во менаџмент инфраструктура  
05.08.2019 - Завршена имплементација на надградби и закрпи во клиентска инфраструктура Надворешни линкови HPE -

---

[2][https://support.hpe.com/hpsc/doc/public/display?docLocale=en\\_US&docId=emr\\_na-hpesbhf03933en\\_us](https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03933en_us)  
VMware - [3]<https://www.vmware.com/security/advisories/VMSA-2019-0008.html>  
Microsoft -  
[4]<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv190013>

[1] <https://kb.vmware.com/s/article/68024>  
[2] [https://support.hpe.com/hpsc/doc/public/display?docLocale=en\\_US&docId=emr\\_na-hpesbhf03933en\\_us](https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03933en_us)  
[3] <https://www.vmware.com/security/advisories/VMSA-2019-0008.html>  
[4] <https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv190013>