Заштита на neoCloud од Downfall безбедносни напади

05/17/2024 04:37:10

FAQ Article Print

Category:	General	**Votes:**	0
State:	public (all)	**Result:**	0.00 %
Language:	mk	**Last update:**	11:55:09 - 08/16/2023

Keywords

Security Downfall

Symptom (public)

Problem (public)

На 08.08.2023 компанијата Intel објави безбедносни пропусти во голем број од процесорите кои се актуелни на глобално ниво, од Intel Scalable серверските процесори до Intel Core, Atom и други клиентски процесори. Downfall нападите овозможуваат преземање на податоци од други корисници кои делат компјутер или, кај cloud инфраструктури, преземање на податоци од други корисници кои го делат истиот сервер.

Повеќе информации за безбедноniот пропуст и нападите може да се најдат на следните линкови:
[1]Downfall
[2]INTEL-SA-00828
[3]INTEL-SA-00813

[1] https://downfall.page/
[2] https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00828.html
[3] https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00813.html

Solution (public)

Заштита на инфраструктурата на neoCloud Во инфраструктурата на neoCloud која се користи за клиентските виртуелни машини се користат процесори кои се афектирани од безбедносните пропусти. Заштитата на инфраструктурата на neoCloud подразбира инсталација на microcode update, односно надградба на SystemROM на серверите со неодамна објавените верзии кои ги затвораат безбедносните пропусти.

Инфрастурктурата на neoCloud за управување со платформата не користи процесори кои се афектирани од безбедносните пропусти.

Покрај инсталација на microcode update, не се потребни дополнителни активности на платформата за виртуелизација, системите за управување или оперативните системи на клиентските виртуелни машини. Преземени активности 16.08.2023 - Креирање на иницијалниот документ, информирање и анализа за влијание и одредување на патека за резолуција