# Protecting neoCloud against Downfall security attacks

05/12/2024 12:37:23

**FAQ Article Print**

| | | | |
|---|---|---|---|
| **Category:** | General | **Votes:** | 0 |
| **State:** | public (all) | **Result:** | 0.00 % |
| **Language:** | en | **Last update:** | 12:08:16 - 08/16/2023 |

***Keywords***

Security Downfall

***Symptom (public)***

***Problem (public)***

On 08.08.2023 Intel published a series for security vulnerabilities affecting modern processors which are widely used globally, from Intel Scalable server processors to Intel Core, Atom and other client processors. Downfall attacks can be used to steal sensitive information and data from other users who share a computer or, in cloud infrastructures, steal data from other customers who share the same server.

Additional information on the security vulnerability and attacks can be found on the following links:
[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)***

Protecting neoCloud infrastructure In neoCloud's infrastructure that host the tenants' virtual machines we use processors which are affected by the security vulnerabilities. Protection of the infrastructure means installation of a microcode update, i.e. upgrade of the SystemROM on the servers with the recently published version which mitigate the security vulnerabilities.

The infrastructure for managing neoCloud's platform is not affected by the security vulnerabilities.

Besides installation of the microcode update, no additional activities are necessary on the virtualization platform, management systems or operating systems on the clients' virtual machines. Undertaken actions 16.08.2023 - Creation of initial document, information and analysis on impact and determining a path for resolution.