Meltdown and Spectre vulnerability

Jan 12

2018

Product Security Advisory

Product Security Advisory: Meltdown and Spectre vulnerability in Common Product Platforms (CPP)

Background:

In December 2017 information about two vulnerabilities in modern processors were published. These exploits are often referred to as Meltdown and Spectre. Due to the nature of the flaw, many processors (AMD, ARM, Intel, etc.) are considered vulnerable.

In order to use the exploit, an attacker needs to execute malicious code on the target system. It is thus generally advised to protect systems from unauthorized access (e.g. by using a strong password policy).

Our IP cameras and encoders are based on Common Product Platform (CPP) designs. Each CPP uses a specific System-on-Chip (SOC), or a family of SoC's, which inherit various CPU cores. Some of them include ARM cores, which are considered vulnerable.

We therefore have analyzed our Common Product Platforms if they are affected, with the result:

- Our Common Product Platforms CPP-ENC, CPP3 and CPP4 are not affected by the vulnerabilities.
- The processors used in the SoC's of our Common Product Platforms CPP6, CPP7 and CPP7.3 are affected. But as we do not allow 3rd party code being installed or executed on our cameras, successful exploitation is considered not possible with Meltdown or Spectre.

In short, our IP cameras and encoders are not vulnerable to Meltdown or Spectre exploitations.

To endure insusceptibility it must be ensured to have recent firmware installed on the devices and access protection kept on a reasonable level.