CERT-EU Security Advisory 2017-025

Critical Vulnerabilities Affecting Intel Firmware

November 21, 2017 — v1.0

History:

• 21/11/2017 — v1.0: Initial publication

Summary

On the 20th of November 2017, Intel reported that it has identified security vulnerabilities that could potentially impact various product families of processors [1].

The following components are affected:

• Intel® Management Engine (Intel® ME)
• Intel® Trusted Execution Engine (Intel® TXE)
• Intel® Server Platform Services (SPS)

Technical Details


As the result of the above mentioned vulnerabilities, an attacker could gain unauthorized access to platforms by impersonating the Intel Engines and platforms, it can execute arbitrary code or cause system crash. Apparently, the attacks can be conducted even when a computer is powered off [5].

Products Affected

Systems using Intel ME Firmware versions 11.0.0 through 11.7.0, SPS Firmware version 4.0, and TXE version 3.0 are impacted. Specific firmware versions on certain Intel processors families:

• 6th, 7th, and 8th generation Intel® Core™ Processor Family
• Intel® Xeon® Processor E3-1200 v5 and v6 Product Family
• Intel® Xeon® Processor Scalable Family
• Intel® Xeon® Processor W Family
• Intel Atom® C3000 Processor Family
• Apollo Lake Intel Atom® Processor E3900 series
• Apollo Lake Intel® Pentium® Processors
• Intel® Celeron® N and J series Processors

Recommendations

• Follow the detection and mitigation procedure described in the Recommendations section of the original Intel advisory [2].
• Use Intel detection tool to analyze your systems for the vulnerabilities [3].
• Follow Intel recommendations on checking with system OEMs for updated firmware [4].

References