CONNECT | MANAGE | PROTECT

INTEL CPU MELTDOWN AND SPECTRE IN GILAT SYSTEMS

Analysis Report

January 2018

Tulsa | Washington, D.C. | Atlanta | Chicago | Philadelphia
866.480.2263 | www.sagenet.com

SageNet
CONNECT | MANAGE | PROTECT

CONTENTS:

CHAPTER 1: INTRODUCTION

Purpose of This Document

This document provides a brief description of the two microprocessor architectural flaws that were discovered recently.

The document then describes the effect, if any, on the Gilat's systems that are based on the x86 CPUs. The future steps for monitoring architectural flaws are listed at the end of the document.

As described in the document, these microprocessor architectural flaws do not affect any Gilat platforms. Thus, SageNet's customers can rest easy knowing that their VSAT Customer Premises Equipment and Management Servers are not susceptible to Meltdown and Spectre vulnerabilities.

What are Meltdown and Spectre?

Meltdown (security vulnerability) definition from Wikipedia, the free encyclopedia:

Meltdown is a hardware vulnerability affecting Intel x86 microprocessors and some ARM-based microprocessors. It allows a rogue process to read all memory, even when it is not authorized to do so.

https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)

Spectre (security vulnerability) definition from Wikipedia, the free encyclopedia:

Spectre is a vulnerability that affects modern microprocessors that perform branch prediction On most processors, the speculative execution resulting from a branch misprediction may leave observable side effects that may reveal private data to attackers. For example, if the pattern of memory accesses performed by such speculative execution depends on private data, the resulting state of the data cache constitutes a side channel through which an attacker may be able to extract information about the private data using a timing attack.

https://en.wikipedia.org/wiki/Spectre_(security_vulnerability)

CHAPTER 2: GILAT SYSTEMS RELATED TO MELTDOWN AND SPECTRE ISSUES

The Gilat runs several functions over Intel x86 CPUs.

These functions are divided into two types:

- **Real Time embedded**
  - In SkyEdge II-c, these servers are based on vanilla kernel of Linux
  - In SkyEdge and SkyEdge II, these servers are based on VxWorks
- **Management Servers**
  - In SkyEdge II-c, these servers are based on industry Linux distributions and Windows (for UTS only)
  - In SkyEdge and SkyEdge II, these servers are based on Windows

For its **Real Time** x86 and **Management** servers, Gilat uses in-house software and auxiliary software packages.

Gilat's system is a closed garden system, which executes only verified SW that is installed by Gilat.

In order to use Meltdown and Spectre, the attacker needs to run unverified software on the attacked machines, sharing the same CPU with the operational software.

This is relevant to the cloud environment where VMs used by different customers run on the same physical machines.

Gilat's servers, both Real Time embedded and non-real time Management, use only the software and applications installed by Gilat or provided by Gilat.

Gilat's VSAT platforms and VSAT MEC run only Gilat's proprietary software and do not allow executing external application.

Hence, the aforementioned flaws are irrelevant to all Gilat platforms.

CHAPTER 3: NEXT STEPS

As mentioned earlier, these vulnerabilities exploit CPU architecture flaws, not operating system. There are certain OS/CPU combinations that offer security patches and will offer more in the near future.

Each of the patches that are found relevant to Linux distribution and used in Gilat's system will be examined over time by Gilat to determine necessity and compatibility with Gilat's application.

ABOUT SAGENET

SageNet designs, implements, manages and protects fast, secure and reliable networks that empower organizations to achieve their core business objectives.

SageNet's integrated network infrastructure, dedicated personnel and innovative products and services suite have set the standard for Managed Network Services and Cybersecurity Solutions. Combining longstanding traditions of industry leadership, innovation and a passionate commitment to customer support, SageNet manages communications at more than 160,000 locations. The company's customer base represents many of the nation's leading retail, healthcare, financial and energy companies, as well as public utilities, state lotteries and government agencies.

Today's SageNet offers a uniquely broad and deep understanding of local and wide area network technologies and leading-edge cybersecurity solutions, all backed by a nationwide field service organization and three 24/7 U.S.-based Network and Security Operations Centers.

Headquartered in Tulsa, SageNet also has regional offices in Washington, D.C., Atlanta, Chicago and Philadelphia.