Meltdown & Spectre

by Robert Hawk

xMatters Information Assurance (IA) team
Tuesday 30 October 2018

Introduction

In January 2018, Google LLC released an advisory which became known as the Meltdown and Spectre vulnerabilities. A website for the Meltdown and Spectre vulnerabilities was setup at Graz University of Technology. Currently, xMatters has no known cybersecurity risks and/or issues in regard to the Meltdown and Spectre vulnerabilities.

Meltdown and Spectre

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware bugs allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.

Source: https://meltdownattack.com/

Risk due to Vulnerability

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system.

Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre.

Source: https://meltdownattack.com/

Risk Management

xMatters Risk Management, Cybersecurity and Engineering teams have investigated the risks posed by Meltdown and Spectre vulnerabilities:

1. Information presented by authoritative sources was reviewed and analyzed in regard to xMatters systems and operations.
2. Investigation and tests were conducted on xMatters systems to determine the existence of the vulnerabilities, the exposure to the vulnerabilities, and any possible attack vectors against xMatters systems.
3. xMatters engineering conducted patches of affected systems within xMatters co-located datacenter infrastructure.
4. xMatters Software as a Service (SaaS) has begun a migration from co-located datacenters to Google Cloud Platform (GCP) Infrastructure as a Service (IaaS). The Google Cloud Platform IaaS is one of the first large scale infrastructures that was fully patched against the Meltdown and Spectre vulnerabilities.

At this time, xMatters has no known cybersecurity risks and/or issues in regard to Meltdown and Spectre vulnerabilities. xMatters Risk Management, Cybersecurity and Engineering teams will continue to investigate internally as well as monitor industry-based news for any changes or updates in regard to the Meltdown and Spectre vulnerabilities.

Resources

The following websites were reviewed and information was used in regards to xMatters risk management for the Meltdown & Spectre vulnerabilities:

Meltdown & Spectre
https://meltdownattack.com/

Mitre – CVE-2017-5715
www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5715

Mitre – CVE-2017-5753
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5753

Mitre – CVE-2017-5754
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5754

Intel
https://newsroom.intel.com/news/intel-responds-to-security-research-findings/

United States Computer Emergency Readiness Team (US-CERT) Notification
https://www.us-cert.gov/ncas/current-activity/2018/01/03/Meltdown-and-Spectre-Side-Channel-Vulnerabilities

Google's Announcement
https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html