NFOCUS

Response to Meltdown and Spectre

Document Revision 1.1
Date of Issue: 1/4/2018

Author: Craig B. Clawson

Director of Development and Operations

Table of Contents

1. Executive Summary

On January 3rd, 2018, security researchers from Google, Cyberus Technology, Graz University of Technology, and others announced several critical vulnerabilities in modern processors. These hardware bugs allow programs to steal data which is currently processed on the computer.

These vulnerabilities, commonly referred to as “Meltdown” and “Spectre” can affect personal computers, mobile devices, and cloud servers.

However, due to the nature of the attack vector, we do not suspect NFocus customer or stored list data to be at risk from these potential attacks.

NFocus will continue to monitor the situation closely, and have immediately began to apply vendor provided patches to mitigate any potential future risk. Additionally, our existing security policies and procedures ensure that you can trust your business to NFocus.

2. Introduction

NFocus Consulting is a company rooted in strong data, supported by knowledgeable people, and strengthened by innovative solutions to accelerate customer success. That mantra has guided our company since 1989 and is the reason why the top direct marketers, printers, and publishers have chosen to partner with NFocus for their data needs.

Data is the foundation of our success. NFocus is a host site and marketing technology provider for 99.9% of US addresses including the largest saturation, consumer, automotive, and property databases. NFocus provides complete data intelligence with thousands of demographic, financial, transactional, behavioral, and trigger overlay options.

Since our business and customers rely on our data for their success, we treat data security with respect and attention it deserves. We implement a holistic approach to security, and understand that no one technology, process or staff member can secure our data alone.

3. Understanding Meltdown and Spectre

3.1 Meltdown and Spectre defined

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 programs into leaking their data.

3.2 Our approach to Spectre

The attack profile of Spectre is either server to client, or cloud tenant to cloud tenant. Since all NFocus servers are on premises, this eliminates that attack vector from our profile. And, while we are using virtual machine technology in our datacenter, every guest on each server is fully controlled by NFocus, and therefore not at risk of being attacked by a guest machine not controlled by NFocus.

3.3 Our approach to Meltdown

As with Spectre, the attack profile for Meltdown is server to client. This means that, at the time of this writing, our servers are secure from a remote code execution from this vulnerability.

However, we are in the process of deploying vendor supplied patches to both servers and workstations within NFocus to proactively mitigate any attack that might leverage this vector in a remote, client to server exploit. At the time of this writing, no such attack is known.

3.4 Monitoring the situation

Our support and management teams are watching these situations closely, as we do with all security concerns. We will continue to proactively assess, address, and mitigate any security concerns using our established policies and procedures. We have never stopped to treat our client and list data with the privacy and security your business demands.

4. Conclusion

Meltdown and Spectre are critical exploits, and customers should work with their Information Technology teams to ensure end user and cloud-based systems are secure.

The nature of the attack does not put our server software or data at risk, at this time. However, management and Information Technology teams continue to be on the cutting edge of security information to ensure your client and list data remain secure.

Just as threats to security can come from any direction, our response and protection to those threats are multi-directional. By hiring the best people, and leveraging industry best-practices, you should feel at ease ensuring NFocus with your data needs.

Notes and legal

The information contained in this document is for general information purposes only. The information is provided by NFocus Consulting, Ltd, and makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to products or services.

Any agreements made in the Master Services Agreement (MSA) made between your company and NFocus will take precedence over any information in this document.

This document is the intellectual property of NFocus Consulting, Ltd, and should be distributed in any form without the permission of NFocus consulting personnel. Distribution of this document without NFocus written permission could be seen as a violation of our Master Non-disclosure agreement, and may result in legal action.

Intel, Google, Microsoft, and other company names are the property of the respective copywrite holders.