Virtual Instruments Vulnerability Statement

Product Impacts from CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754
January 04, 2018 - Document Version 1.0

Virtual Instruments has analyzed CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754 also known as "Meltdown" and "Spectre". This document provides customers with additional information on the exposure, exploitability of and remediation for Virtual Instruments products.
This notification will be revised as more information becomes available.

Impact

Allows unprivileged code to read memory of both the kernel and other applications. This is a vulnerability in the system processor used in all VirtualWisdom Performance Probes and Platform Appliances as well as LoadDynamiX Enterprise and Load Generation Appliances. Because VirtualWisdom and LoadDynamiX are closed systems, and do not allow arbitrary code execution, there are no known ways to exploit these processor vulnerabilities with physical appliances and probes. Exploitation would require leveraging an additional, unknown vulnerability that tricks the appliance into running code provided by the attacker. The attacking code need not be run with elevated privileges.

Virtual Instruments products exposed but not vulnerable

VirtualWisdom Platform Appliance 4210 and 4220 – all software versions and virtual editions
VirtualWisdom SAN Performance Probe Family – all firmware versions

- ProbeFC8
- ProbeFC8-HD
- ProbeFC8-HD48
- ProbeFC-16G-24
- ProbeFC-16G-12

VirtualWisdom NAS Performance Probe – all firmware versions
LoadDynamiX Enterprise - all firmware versions (2.0 - 5.4)
LoadDynamiX Load Generation Appliances - all firmware versions

- 1G/10G/FC/Unified Series
- 32GFC/25GbE/40GbE Series
- Sensor

LoadDynamiX Test Development Environment - unaffected

Virtual Instruments products exposed and vulnerable

VirtualWisdom Platform Appliance – all virtual editions
Xangati Management Appliance – all virtual editions
LDX-V – all virtual appliances
LDX-VLS – Virtual Appliances License server – all releases

Remediation

For Virtual Editions, we recommend that all customers contact the vendors of their virtualization platforms to obtain patches to protect Virtual Instrument's virtual editions from vulnerabilities at the hypervisor layer.

Our upstream OS vendors are testing patches that work around the processor vulnerability, and expect to release them shortly or have already released them.

Virtual Instruments will incorporate these OS patches into patches for our latest software and firmware versions and publish performance and functionality impacts from our qualification processes.

Additional Information

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5753
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5715
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5754