SECURITY BULLETIN: MOBILE ASPECTS PRODUCTS EXPOSE TO MELTDOWN AND SPECTRE VULNERABILITIES

SUMMARY

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. See Reference links below for more information.

VULNERABILITY DETAILS

Meltdown
CVEID: CVE-2017-5754
Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache. See Reference link for a list of all vulnerable processors.

Spectre
CVEID: CVE-2017-5753 and CVE-2017-5715
Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

AFFECTED PRODUCTS AND VERSIONS

All cabinets that are equipped with Intel i5 CPU M520 processors are impacted by these vulnerabilities. This includes:

iRIScope 2.0

iRISupply 4.0 (upgrade), 5.0

REMEDIATION/FIXES

The recommended solution is to apply the appropriate patches for this vulnerability.

Operating System Update

Windows 10

- version 1507 — KB4056893 (issued 1/3/18)
- version 1511 — KB4056888 (issued 1/3/18)
- version 1607 — KB4056890 (issued 1/3/18)

- version 1703 — KB4056891 (issued 1/3/18)
- version 1709 — KB4056892 (issued 1/3/18)

Windows 7 and Windows Server 2008

- Windows 7 SP1 and Server 2008 R2 SP1 — KB4056897 (Security only, issued 1/3/18)
- Windows 7 SP1 and Server 2008 R2 SP1 — KB4056894 (Monthly rollup, issued 1/4/18)
- No patches available for Windows Server 2008 non-R2 version

BIOS Micro-Code Update

Mobile Aspects works closely with Advantech Corporation to assemble the hardware components for our products. As of now, there are no new micro-code patch solutions. However, Advantech is continuously working with Intel to get latest patches.

Cloud Services

Mobile Aspects works closely with third party cloud services to support our internal infrastructure. As of now, there are no new patch solutions.

REFERENCES

Overview - https://meltdownattack.com

Overview (2) - https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html

List of vulnerable processors - https://www.techarp.com/guides/complete-meltdown-spectre-cpu-list/

CHANGE HISTORY

January 23, 2018: Original version published.