April 2, 2018

Dear Valued Harmonic Customers,

As many of you are likely aware, two major system vulnerabilities known as *Spectre* (CVE-2017-5753, CVE-2017-5715) and *Meltdown* (CVE-2017-5754) have been in the news, highlighting security risks for millions of systems around the globe.

Harmonic has reviewed the recent *Meltdown* and *Spectre* patches for risk and impact to Harmonic products, and we would like to provide you with some information on our analysis to date:

- For the products outlined in the list below, we believe at this time the risk of side-channel exploit type attacks is very low. We believe this to be the case as our customers typically keep their Harmonic equipment behind enterprise grade firewalls, hence limited exposure. Additionally, these products typically do not run any third party software on them. Therefore, an immediate installation of patches is not necessary at this time. For future releases of these products, we will consider patches to address side channel exploit vulnerabilities and other vulnerabilities as we currently do as part of roadmap planning.

    - Electra 8000, Electra 9200, ElectraX2, ElectraXVM, Electra VS, Electra XT
    - ProStream 1000/9100, ProStreamX, ProStreamXVM
    - Spectrum, SpectrumX, Spectrum XE
    - ViBE EM1000/2000/4000, CP6000, CP9000
    - ProMedia
    - MAS
    - Amethyst
    - Netprocessor
    - ProView
    - MediaGrid
        - **April 2nd Update: No Change**

- **April 2nd Update**
- Harmonic continues to work closely with our manufacturers (Intel, Dell, HP, etc.) and is aware of the patches that they have made available. At this time, Harmonic is evaluating/testing these patches and strongly recommends **NOT** installing any of them on Harmonic equipment. We will continue to keep our customers informed of progress on this topic.

- For the following products: NMX, WFS, Carbon, Polaris, XMS, DMS, Electra X2S, System Manager, Sapphire, Edge MS and MediaGrid FSD Client, we are currently testing the impact of Operating System patches on Harmonic software. At this time, Harmonic does not recommend installing Microsoft patches on these (Windows-based) systems until our testing is completed.
    - **April 2nd Update: Work in Progress.**

- For VOS-based products on public cloud, private cloud or on appliances, we have determined that these products also need to apply the relevant patches and are currently testing an updated software package to ensure everything functions as intended. These products include:

    - VOS Cluster
    - VOS 360

- - CloudLinks
  - VOS Engine
    - **April 2nd Update: Work in Progress.**

- Harmonic has contacted our public cloud vendors who have already patched their infrastructure for the vulnerabilities. If you use cloud infrastructure not provided by Harmonic, please contact your infrastructure provider.

- For CableOS, much like our appliances, we believe that in general, the risk of these vulnerabilities is low.
  - Harmonic has also assessed the risk of performance degradation that may be caused by Linux OS patches intended to address these vulnerabilities (once the patches are formally made available). Our assessment is as follows:
    - The Linux OS patches are expected to have very minimal impact on processing tasks which bypass the Linux kernel.
    - Given that most of the heavy-duty processing of CableOS indeed bypasses the kernel, we expect that any negative impact on CableOS performance will be minimal.
    - As soon as these relevant OS patches become available, Harmonic will perform thorough benchmarking tests in order to quantify (and minimize) any impact.
    - Once completed, Harmonic will issue further updates.

As stated above, Harmonic also strongly recommends taking any and all precautions within your IP networks, ensuring that these products are protected behind enterprise grade firewalls. This is a long-standing best practice that will help ensure optimum protection for your systems.

Harmonic will be releasing a follow-up communication on this topic on **May 4, 2018** to provide an update on our testing efforts as well as an update on any further findings on the Intel Spectre/Meltdown vulnerabilities.

If you have further quesitons on this topic, please contact your account team and/or Harmonic Support to discuss.

Best regards,

Harmonic Service & Support