Product Notice #0325

"Spectre" (CVE-2017-5753 and CVE-2017-5715) and "Meltdown" (CVE-2017-5754) Security Vulnerabilities

CPU manufacturers and OS vendors recently announced several vulnerabilities in their products, collectively known as "Spectre" and "Meltdown". The following guidance is given based on our interpretation of these announcements and the limited information available from these suppliers at this time. AudioCodes assumes the information provided by these vendors to be complete and accurate.

Executive Summary

Our current analysis of these vulnerabilities reveals that most of AudioCodes' products are not considered as vulnerable to these attacks. Information and guidance is hereby provided as we continue our investigation.

Detailed Notice

This Product Notice addresses vulnerabilities CVE-2017-5753 and CVE-2017-5715, which are collectively known as "Spectre", and CVE-2017-5754, which is known as "Meltdown".

The reported security vulnerabilities affect microcomputer systems that use speculative execution. The reported vulnerabilities may permit an unprivileged local attacker, in specific circumstances, to read privileged memory belonging to other processes or to memory allocated to the operating system kernel.

As reported, the attacker must be able to insert and execute malicious code on the attacked target system or host (in a virtualized environment). It now appears that only devices or environments that allow non-trusted third-parties to execute their customized code side-by-side with AudioCodes' code on the same microprocessor or host, may be considered vulnerable.

Most AudioCodes' products are closed and do not allow external third-party code to run on the products. In other words, almost all AudioCodes hardware products, including the Mediant SBCs, Media Gateways and IP Phones do not allow execution of any customized user code on the device and thus, are not affected by the reported vulnerabilities.

AudioCodes software products that are deployed as virtual machines on shared hosts, although not directly affected by any of these vulnerabilities, could be targeted by such attacks if the hosting environment is vulnerable. AudioCodes recommends that customers update their underlying virtual host with the security updates provided by their respective host vendors.

AudioCodes advises its Customers to follow the below general guidelines:

a. A user with access to AudioCodes systems is intended to be one that is trusted by the local administrator.

b. We recommend customers to continue to follow our existing security recommendations regarding each product.

For the following products, Customers are further advised to apply the latest operating system security updates as they become available by AudioCodes:

- CloudBond™ 365 Standard/ Standard+ Edition
- CloudBond 365 Pro Edition
- CloudBond 365 Enterprise Edition
- CloudBond 365 Standard CCE
- CloudBond 365 Enterprise CCE
- Mediant 800 SBA / SBA-N
- Mediant 1000B SBA / SBA-ES / SBA-EO
- Mediant 2600B SBA
- OVOC Server

AudioCodes products that are not listed above are currently not considered as affected by the vulnerabilities.

AudioCodes is working with its software and hardware partners to evaluate relevant software and firmware updates as they become available.

Legal Disclaimer

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. AUDIOCODES RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME. AUDIOCODES EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE

If you have any questions, at https://www.audiocodes.com/corporate/offices-worldwide

AudioCodes Ltd. | 1 Hayarden Street | Airport City | Lod | Israel | +972-3-976-4000