VIVOTEK Product Security Advisory

Advisory ID: VVTK-SA-2018-001
CVE ID: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

First Published: January 10, 2018
Last Update: January 10, 2018
Status: Confirmed
Revision: 1

Overview:

Unauthorized information disclosure through CPU side-channel attacks ("Meltdown" and "Spectre").

Details:

More information of the "Meltdown" and "Spectre" vulnerabilities can be found at the following URLs:
https://meltdownattack.com/
https://googleprojectzero.blogspot.co.at/2018/01/reading-privileged-memory-with-side.html

VIVOTEK products are based on a number of different CPU architectures, some of which are affected by the vulnerabilities. However, no arbitrary code can be executed by unauthorized users on our product.

NVRs:

ND Series: Not affected by the vulnerabilities because users are not allowed to execute any program in our systems.

NR Series: Users have the completed authorization to system administration. Therefore, the vulnerabilities do not cause any data leak or unauthorized access.

Network Cameras:

Not affected by the vulnerabilities because users are not allowed to execute any program in our systems.

Affect Products:

Vulnerable Products:

NVR - NR9581, NR9681

Products Confirmed Not Vulnerable:

NVR - ND Series

Network Cameras - All Series

Workarounds:

No workarounds required.

Solution:

No immediate action is required.

VIVOTEK will keep investigating kernel patches, CPU microcode and other mitigations. The known mitigation techniques would largely reduce the CPU efficiency. VIVOTEK will release the version update after we complete the tests and apply the least effect on CPU.

Revision History:

Revision 1 / January 10, 2018 / Initial release