open-e

Open-E, Inc.
2820 Lassiter Rd., Building C
Marietta, GA 30062
United States of America

Phone: +1 (678) 666 2880
Email: info@open-e.com

www.open-e.com

To whom it may concern

Marietta, GA – January 15, 2018

Statement on "Meltdown" and "Spectre" vulnerabilities

Meltdown and Spectre are hardware-based vulnerabilities, affecting processors which allow unauthorized users access to kernel space by locally running exploits in the form of binary files.

Because Open-E Data Storage Software is a closed environment, none of the DSS family products is vulnerable to attacks using Meltdown and Spectre exploits. In our products, each and every step of their configuration, and while using them, users cannot run any processes.

During the whole contact with our product – from the installation process to day-to-day work – users are incapable of running unauthorized processes of any kind. They can benefit from the complete set of product functionalities while all processes created by Open-E's developers run in a separate layer where modification of any kind is impossible.

Please be informed that in case Open-E Data Storage Software is running in a virtual environment, a Meltdown or Spectre attack may be possible because of 3rd party Hypervisor vulnerabilities. We strongly advise to install the latest CPU security patches on Hypervisor machines.

One of Open-E's top priorities is the safety of our customers and their data. This is why, apart from providing you with a product environment that is invulnerable to direct attacks, we plan to release additional kernel patches in upcoming product releases.

Janusz Bak
Chief Technical Officer

Todd Maxwell
Vice President of Global Support
and Technical Sales