ExaGrid Statement on Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5753 & CVE-2017-5715)

Date: 1/8/2018

Applicability: All ExaGrid Appliance Models

ExaGrid's platform engineering team has carefully analyzed the recent malicious exploits known as Meltdown and Spectre and their potential impact on ExaGrid's family of hyper-converged secondary storage for backup appliances.

It is important to note that ExaGrid appliances, unlike a general-purpose system, are purpose-built, closed systems with tight control over the set of applications and executed code. ExaGrid appliances do not run unknown user space code, which is a key element of these vulnerabilities.

By following ExaGrid's best practices on securing the ExaGrid appliances, the attack surface for these exploits is minimized because without network or local access to the ExaGrid appliance, there is no way to inject or run the user space code necessary to exploit these vulnerabilities.

Your ExaGrid customer support engineer can work with you to review the following best practices:

1. Non-default passwords for administrator and support accounts
2. IP-based white lists controlling share access with optional SMB signing
3. Use of ExaGrid audit log to monitor GUI access

ExaGrid remains committed to the security and safety of its products. We are working closely with our vendors to identify the proper patches and updates, and to ensure any performance impact of such updates are fully understood. We will continue to keep you informed about the impact of these exploits on your ExaGrid appliances.