DDN STORAGE

TECHNICAL SUPPORT BULLETIN

DDN TECHNICAL SUPPORT | SPT-TSB-0088 (A3) | 15 JANUARY 2018

SECURITY ALERT

Meltdown and Spectre Vulnerabilities in Intel, ARM, AMD and IBM Power Processors

ALERT! **Customers should NOT attempt to patch their DDN storage systems or software** for Meltdown or Spectre on their own. DDN cannot guarantee its products will function if a user patch is attempted.

Issue Summary

Security vulnerabilities in the fundamental design of Intel, ARM, AMD, and IBM Power processors have recently been publicized in the trade press under the names "Meltdown" and "Spectre". The vulnerabilities are side-effects of features designed to speed process execution. Consequently, any mitigation is likely to have a negative impact on performance.

- **Meltdown (CVE-2017-5754)** — Meltdown has been described as a kernel leak vulnerability and a rogue data cache load vulnerability. Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache. The vulnerability is exposed to any operating system in which privileged data is mapped into virtual memory for unprivileged processes (a common practice). This vulnerability was first reported in 1995 by the US National Security Agency. It is rated difficult to exploit by the National Vulnerabilities Database of NIST (the US National Institute of Standards and Technology), with an exploitability rating of 1.1 on a scale of 1 to 10. The impact if exploited is considered moderate (rating 5.6 on a scale of 10).

- **Spectre (CVE-2017-5753, CVE-2017-5715)** — Spectre has been described as a kernel speculative execution vulnerability. It actually consists of two vulnerabilities: a bounds check vulnerability and a branch target injection vulnerability. Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. Although currently believed to be exploitable only by user programs, Spectre can allow malicious programs to induce a hypervisor to transmit data to a guest system running on top of it. Like Meltdown, Spectre is rated difficult to exploit by the National Vulnerabilities Database of NIST, with an exploitability rating of 1.1 on a scale of 1 to 10. The impact if exploited is considered moderate (rating 5.6 on a scale of 10). Spectre is considered the more difficult of the two vulnerabilities to mitigate.

An important aspect of these vulnerabilities is that they require malware to run locally on a system in order to exploit them. They do not expose a new vector for remote attack. There have been no known attacks leveraging the Meltdown or Spectre vulnerabilities.

Affected Systems and Software

All DDN products incorporate or execute on affected processors and are therefore vulnerable to Meltdown and Spectre. DDN product performance may be affected by workarounds to mitigate these security vulnerabilities.

Resolution

True resolution of the Meltdown and Spectre security vulnerabilities would require processor redesign and replacement by the chip manufacturers. However, the vulnerabilities can be mitigated significantly in software. Effective mitigation requires changes to CPU and BIOS firmware, operating system software, and I/O drivers used by DDN products. Most major Linux distributions have fixes available now or forthcoming shortly. However, drivers will take some time to become available. Spectrum Scale and Lustre file system software must then be modified to accommodate these changes.

Due to the complexity of the interactions among these components in DDN products, DDN will address Meltdown and Spectre by means of ***full software or firmware upgrades only***. No patches will be issued.

Upgrades addressing the Meltdown and Spectre vulnerabilities will be released over the next several quarters for all currently supported DDN product lines.

ALERT! **Customers should NOT attempt to patch their DDN storage systems or software** for Meltdown or Spectre on their own. DDN cannot guarantee its products will function if a user patch is attempted.

Performance Impacts

Preliminary benchmarks reported in the press suggest potential performance degradation of 5% to 45% for Meltdown and Spectre mitigation. Performance impact appears to be sensitive to workload and computational environment, with the biggest performance impacts reported in virtual hosting environments and in random I/O workloads. However, DDN's products and their typical applications do not match any of the tested environments.

Consequently, as Meltdown and Spectre fixes are rolled out, DDN will conduct benchmarks to determine whether, and to what degree, product performance may be affected by the implementation of these security mitigations. If optimizations in the RAID engine or elsewhere can offset performance impacts due to Meltdown and Spectre mitigation, we will make those optimizations in a deliberate, planned manner after the security vulnerabilities are resolved. The net performance impact that customers can expect, as well as any configuration changes that might be helpful, will be described in future Technical Support Bulletins or the product release notes.

Minimizing Exposure

To minimize their immediate exposure to Meltdown and Spectre, DDN recommends that customers follow industry best practices to secure their systems from malicious code execution. Access to the shell execution environment should be restricted. Default user and administrator passwords should be changed and root access passwords should be made more secure. Site security practices should be reviewed and local, physical access to the system should be limited to trusted personnel.

Contacting DDN Technical Support

Please contact DDN Technical Support at any time if you have questions or require assistance. Support can be reached by phone, by email, or on the web as listed below.

Web	
DDN Community Support Portal	https://community.ddn.com/login
Portal Assistance	webportal.support@ddn.com
Telephone	
DDN Support Worldwide Directory	http://www.ddn.com/support/contact-support
Email	
Support Email	support@ddn.com
Bulletins	
Support Bulletins	http://www.ddn.com/support/technical-support-bulletins
End-of-Life Notices	http://www.ddn.com/support/end-of-life-notices
Bulletin Subscription Requests	support-tsb@ddn.com