Security Advisory- Meltdown and Spectre Vulnerabilities – Updated January 7, 2018

Subject: Meltdown and Spectre vulnerabilities – Updated January 7, 2018

Overview

Ex Libris is aware of the recently reported security vulnerabilities known as 'Meltdown' and 'Spectre' that affect computer processors (CPUs). These are vulnerabilities at the architecture level and affect any computer or device, whether running Windows, OS X, Android, iOS or other operating systems. These vulnerabilities can allow a rogue process to access other processes and memory running on the same device. Ex Libris will continue to monitor the issue and provide updates as appropriate.

Meltdown affects Intel processors.

Spectre affects Intel, AMD, and ARM processors.

Effective Security Severity Level:

High

Affected Systems:

All servers.

Actions Taken for Cloud/Hosted Systems:

- Our Security team is monitoring the information that is released around the affected hardware, and we have evaluated Ex Libirs' cloud exposure.
- Our security team applied security reinforcement and protection measures according to our security best practices, in order to help mitigate these vulnerabilities. We have updated our security infrastructure, such as firewalls and intrusion detection and protection tools, with the most updated signatures (CVE 2017-5715, CVE 2017-5753, CVE 2017-5754) that allow us to identify and block these vulnerabilities.
- Since there are industry reports indicating a potential performance impact associated with some of the hotfixes and patches, our Cloud Operations team is testing and certifying the applicable hotfixes and patches before they are deployed to our cloud infrastructure. We are making this testing and deployment activity a major priority.
- Ex Libris customers are protected through the combination of the above-mentioned updated security signatures as well as the overall security mechanisms already in use in our cloud infrastructure, including network segregation and intrusion detection and prevention, as well as proactive security monitoring.
- Ex Libris will continue to monitor the issue and provide updates as appropriate.

Required Actions for On-Premises and Local Systems:

Ex Libris recommends following your vendor's instructions. Refer to your OS vendors for the most recent information. The table provided below lists available patches, but check with your vendors for any updates. Because the vulnerability exists in CPU architecture rather than in software, patching may not fully address these vulnerabilities in all cases.
After patching, *performance maybe reduced by up to 30 percent*. Administrators should monitor applications and services, and work with their vendor(s) to mitigate the effect if possible.

Further Information:

Link to Vendor Patch Information	Date Added
Amazon	January 4, 2018
AMD	January 4, 2018
Android	January 4, 2018
ARM	January 4, 2018
CentOS	January 4, 2018
Chromium	January 4, 2018
Citrix	January 4, 2018
F5	January 4, 2018
Google	January 4, 2018
Huawei	January 4, 2018
IBM	January 4, 2018
Intel	January 4, 2018

Link to Vendor Patch Information	Date Added
Lenovo	January 4, 2018
Linux	January 4, 2018
Microsoft Azure	January 4, 2018
Microsoft Windows	January 4, 2018
NVIDIA	January 4, 2018
OpenSuSE	January 4, 2018
Red Hat	January 4, 2018
SuSE	January 4, 2018
Trend Micro	January 4, 2018
VMware	January 4, 2018
Xen	January 4, 2018