High Security Vulnerability - VENOM Vulnerability (CVE-2015-3456)

- **Product:** Aleph
- **Product Version:** 20, 21, 22, 23
- **Relevant for Installation Type:** Dedicated-Direct, Direct, Local, Total Care

Description

Overview:

Ex Libris has been made aware of a recently discovered vulnerability issue with VENOM rated as “High”.

A privileged guest user could exploit this flaw to crash the guest VM using a ‘buffer overflow’ vulnerability affecting the Floppy Disk Controller (FDC) emulation or, potentially, break free of an affected VM and execute code on the host itself. An attacker could also potentially access data or execute code on other guest VMs running on the same host system.

This vulnerability is only an issue if untrusted access is obtained by a privileged guest user.

This vulnerability is covered by Red Hat advisory CVE-2015-3456 where more information is available.

Additional references:

More detailed analysis of this vulnerability is available from:
• https://access.redhat.com/articles/1444903
• https://fortune.com/2015/05/13/venom-vulnerability/
• http://www.theregister.co.uk/2015/05/13/heartbleed_eat_your_heart_out_venom_vuln_poiso ns_countless_vms/

Effective Security Severity Level: High

Affected Systems: Ex Libris products running on a VM hypervisor known as Quick Emulator (QEMU), which is used in a number of common virtualization products, including XEN hypervisors, KVM, Oracle VM VirtualBox, and the native QEMU client.

Tests and Certifications: Ex Libris has evaluated the risks of this vulnerability. At this point, there is no vendor exploit to this vulnerability. In order to mount an exploit attempt, a user on the guest machine would need sufficient permissions to access the floppy disk controller I/O ports. For Linux guests, that means the user would need to have root access or otherwise elevated privileges. This fix should be installed at the infrastructure level as per vendor recommendations.

Actions Taken for Hosted Systems: Ex Libris has completed the vulnerability assessment and investigation process for potentially affected Hosted systems. This vulnerability exploitation method with Ex Libris cloud design and topology, Ex Libris sees this vulnerability as Low risk. Further update with additional information and mitigation plan will be sent.

Required Actions for On-Premises and Local Systems: Ex Libris strongly recommends following the instructions available from the links listed above and installing the patch on Ex Libris on-premises and local systems, if required.

- **Article last edited:** 16-Mar-2016