Emulex Connectivity Division (ECD) Security Advisory
Emulex Fibre Channel Products

Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method Vulnerabilities (Spectre, Meltdown)

January 22, 2018

Summary:
In total, security researchers disclosed three variants of CPU Data cache timing abuse. The variants lead to vulnerabilities that take advantage of the implementation of speculative execution of instructions on many modern processors to perform side-channel information disclosure. An unprivileged local attacker could read privileged memory belonging to other processes or memory allocated to the operating system kernel.

The three disclosed variants are:
- Variant 1: bounds check bypass (CVE-2017-5753)
- Variant 2: branch target injection (CVE-2017-5715)
- Variant 3: rogue data cache load (CVE-2017-5754)
- Variant 1 and 2 are collectively known as Spectre, the third variant is known as Meltdown.

To exploit any of these vulnerabilities, an attacker must be able to download and run a carefully crafted program on the device.

Products Confirmed Not Vulnerable:
At Broadcom, we are committed to developing technology that supports the industry’s highest security and privacy standards. Broadcom has reviewed our Emulex Fibre Channel (FC) Controllers in production, identified in the table below, with respect to the Spectre and Meltdown vulnerabilities and determined they are not vulnerable.

A list of affected ARM processors, cores has been identified at the link below:

https://developer.arm.com/support/security-update

Broadcom only uses certain ARM-based cores within our Emulex FC Controllers. Broadcom does not use any of the affected ARM cores in any Emulex FC Controllers. The ARM processors used in Emulex FC Controllers are not affected by the Meltdown and Spectre vulnerabilities. These Emulex FC controllers are used in Emulex FC PCIe Host Bus Adapters (HBAs) and various custom form-factor assemblies.

<table>
<thead>
<tr>
<th>Emulex FC Controller Model No</th>
<th>FC Controller Name</th>
<th>Description</th>
<th>Affected by these vulnerabilities?</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOC 540</td>
<td>Saturn</td>
<td>8GFC Controller used in LPe12000-series HBAs</td>
<td>No</td>
</tr>
<tr>
<td>XE201</td>
<td>Lancer G5</td>
<td>Gen 5 16GFC Controller used in LPe15000/LPe16000B-series HBAs</td>
<td>No</td>
</tr>
<tr>
<td>XE501-P1</td>
<td>Lancer G6</td>
<td>Gen 6 32GFC/16GFC Controller used in LPe31000/LPe32000-series HBAs</td>
<td>No</td>
</tr>
</tbody>
</table>

Note:
Unmodified Emulex firmware, drivers, utilities and management software are not vulnerable to Meltdown or Spectre and cannot be used to exploit these vulnerabilities on any components in the system that incorporates Emulex FC products. However, since the system and host operating system that runs Emulex FC products are not under Emulex's control, Emulex recommends customers apply all security advisories from their system vendors.