How to Install the 'Email misuse' Hotfix for local customers

- **Product:** Primo
- **Relevant for Installation Type:** Local

Overview:

A potential misuse of the "Send To Email" functionality in Primo was recently discovered. Below you will find instructions for how to install a Hot Fix for local customers.

Notices:

1. The Hot fix can be installed only on Primo May 2017 Release.

2. The procedure requires to **shutdown** the FE server; therefore, if the installation has more than 1 FE server, it is recommended to run the procedure (steps 1-10 below) on one server at a time to **avoid downtime**.

Step by step instructions:

1. Connect via SSH to Primo FE/s server/s.
2. Type **cd $primo_dev/ng/primo/home/profile/hotfix** and click enter

For Israel and APAC customers:
Type **./getfromftp.sh 20170622134947-EmailSecurityPatchDavid ftp.exlibrisgroup.com primo_hf4 4pgrade** and click enter.

For European customers:
Type **./getfromftp.sh 20170622134947-EmailSecurityPatchDavid ftp.exl.de primo_hf4 4pgrade** and click enter.

For North and South America customers:
Type **./getfromftp.sh 20170622134947-EmailSecurityPatchDavid ftp.exlibris-usa.com primo_hf4 4pgrade** and click enter.

3. Type **primoe** in the console and click enter.
4. Type **primo_shutdown_all** and click enter.
5. Type **cd $primo_dev/ng/primo/home/profile/hotfix** and click enter
6. Type **./inject.sh 20170622134947-EmailSecurityPatchDavid** and click enter

7. Type **cd $primo_dev/system.dir/injection/20170622134947-EmailSecurityPatchDavid/extra_files/sql/** and click enter
8. Type **csh –f be_implementation_note.4.9.10.PRM-35270.csh** and click enter
9. Type **primoe** in the console and click enter.
10. Type **primo_startup_all** in the console and click enter.
11. In Primo Back Office, go to "deploy all" menu and mark **"All Code Tables and Mapping Tables (Front End labels and more)"** as checked and click deploy.