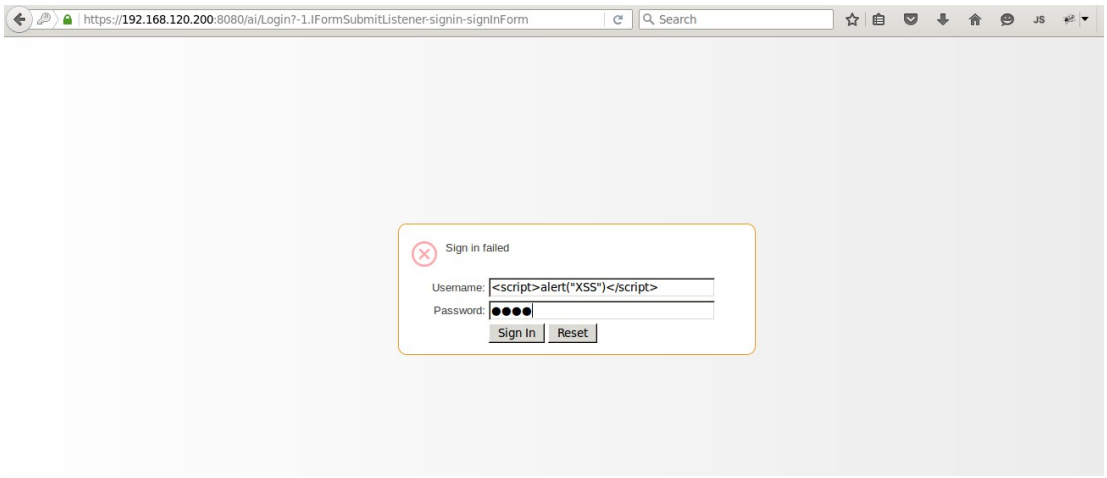
Exploit Title: [CRYPTSHARE – Stored XSS]

Date: [13-May-2016]
Exploit Author: [Luigi Vezzoso]
Vendor Homepage: [https://www.cryptshare.com]
Version: [3.10.1.2]
Tested on: [OPENSUSE 13.2]
CVE : [CVE-2016-XXXX]

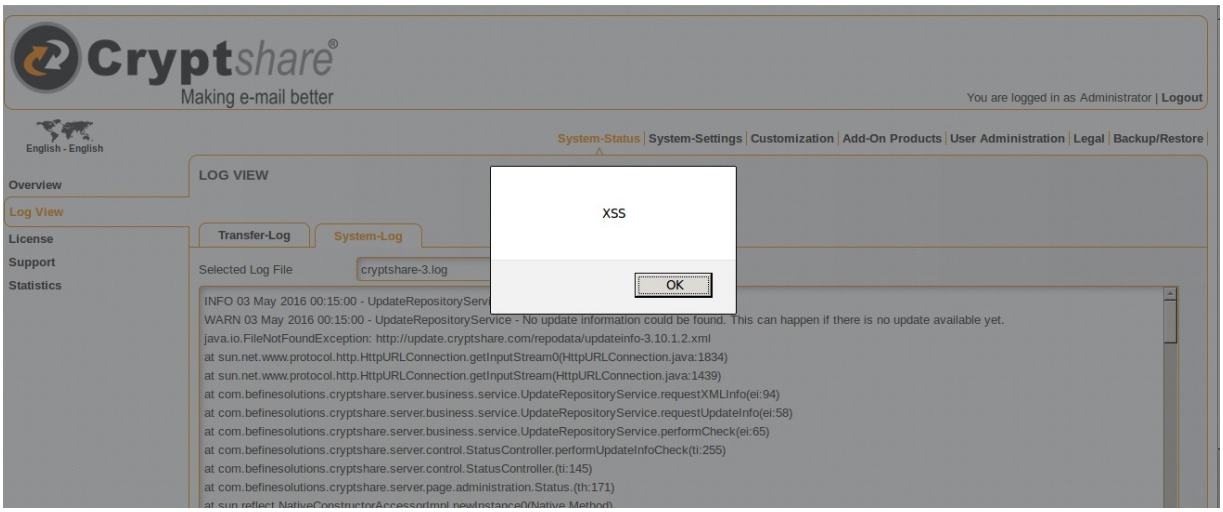
#OVERVIEW
Is possible to inject arbitrary code into the logs simply from the authentication form of the administrative appliance interface. In particular we found the is possible to trigger a stored XSS into the log view interface.

#INTRODUCTION
Cryptshare is a Secure Electronic Communication Solution that enables companies and their staff to exchange encrypted e-mail messages and attachments of any size - at any time, with internal as well as external recipients and directly from your existing e-mail system. There are no special software requirements for the recipients: no user accounts, no certificate exchange or licences are needed. Cryptshare makes it easy to communicate in complete privacy with everyone you need to, instantly, and at any time.

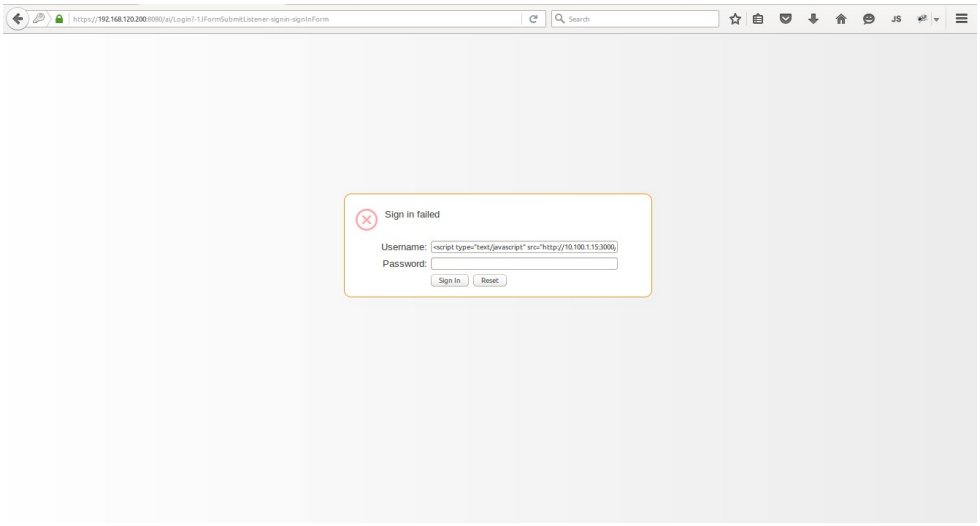
#VULNERABILITY DESCRIPTION
An attacker can inject code from external to the logs from the login form:



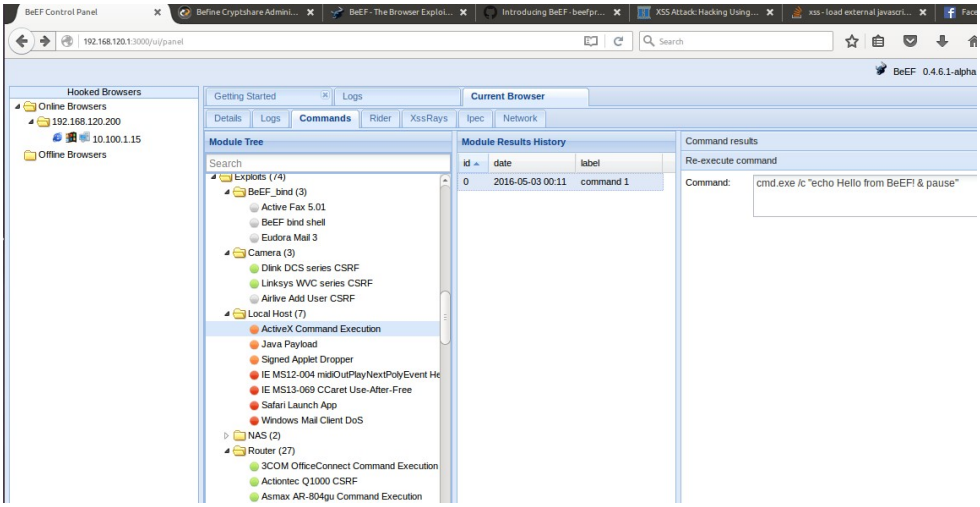
After the injection the XSS is triggered by the Admin simply reading the LOGS:



As an hypothetical attack vector could be the injection of an external Javascript for the BeEF tool. In example we can do:



And finally own the user browser/workstation and launch other attacks.



#VERSIONS AFFECTED
We tested only the last appliance version 3.10.1.2 but also previous versione may be affected too.

#SOLUTION
The vendor have already fixed the issue in the release 3.10.3.1

#CREDITS
Luigi Vezzoso
email: luigivezzoso@gmail.com
skype: luigivezzoso