## # 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:

() () () () () () () () () () () () () (	tener-signin-signInForm	C Search	☆	¢ (	•	俞	ø	JS	≉ •
	Sign in failed								
	$\odot$								
	Username: <script>alert(")</td><td>(SS")</script>								
	Password: ••••	st ]							
	Sign In Res								

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

Cr	' <b>ypt</b> share <sup>®</sup> Making e-mail better You are logged in as Administrator   Logout					
	Making e-mail better You are logged in as Administrator   Logout					
English - English	System-Status   System-Settings   Customization   Add-On Products   User Administration   Legal   Backup/Restore					
Overview	LOG VIEW					
Log View	XSS					
License	Transfer-Log System-Log					
Support	Selected Log File cryptshare-3.log					
Statistics	OK					
	INFO 03 May 2016 00:15:00 - UpdateRepositoryServ					
	WARN 03 May 2016 00:15:00 - UpdateRepositoryService - No update information could be found. This can happen if there is no update available yet. java.io.FileNotFoundException: http://update.cryptshare.com/repodata/updateinfo-3.10.1.2.xml					
	arts of network oundo.coch.http://tlp/IIConnection.get/nput/seam/OHttp/IIC.Connection.java.1834)					
	at sun net. www.protocol.http.http/RLConnection.getInputStream(Http://RLConnection.jexz.1439)					
	at com.befinesolutions.cryptshare.server.business.service.UpdateRepositoryService.requestXMLinfo(ei:94)					
	at com.befinesolutions.cryptshare.server.business.service.UpdateRepositoryService.requestUpdateInfo(ei:58)					
	at com.befinesolutions.cryptshare.server.business.service.UpdateRepositoryService.performCheck(ei:65)					
	at com.befinesolutions.cryptshare.server.control.StatusController.performUpdateInfoCheck(tl:255)					
	at com.befinesolutions.cryptshare.server.control.StatusController.(tl:145)					
	at com.befinesolutions.cryptshare.server.page.administration.Status.(th:171)					
	at sun reflect NativeConstructorAccessoriumi newinstance0(Native Method)					

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