Cure-2013-1008: Security Advisory - Curesec Research Team

1. Introduction

Advisory ID:	Cure-2013-1008
Advisory URL:	https://www.curesec.com/de/veroeffentlichungen/advisories.html
Affected Product:	LiveZilla version 5.0.1.4
Affected Systems	Windows
Fixed in:	5.1.1
Fixed Version Link:	https://www.livezilla.net/downloads/pubfiles/LiveZilla_5.1.1.0_Full.exe
Vendor Contact:	support@livezilla.net
Vulnerability Type:	Local Password Disclosure
Remote Exploitable:	No
Reported to vendor	18.10.2013
Disclosed to public	28.11.2013
Release mode:	Coordinated release
CVE:	CVE-2013-6223
Credentials:	crt@curesec.com

2. Vulnerability Description

An 1click file that allows an admin to log into LiveZilla using a mouse click is saved in a xml representation. This xml file includes the admin username and password in plaintext. Base64 is not an encryption mechanism. If an attacker is able to get access to a 1click file he can easily open the file and discover username and password for an administrator.

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<LiveZilla version="5.0.1.4">
  <server>
    <item lastsiteselected="" httpkeepalive="True" savepassword="True" location="FTPRemote
        "False" autologin="True" selected="False" ftpproxybypasslocal="True" ftpproxyauthe
        False" ftpproxyusername="" ftpproxypassword="" httppassword="RGFpbW[redacted]" htt
        YWRt[redacted]" ftpproxyusage="False" ftpproxyport="3128" autologininstancen
        defaultloginstatus="Online" ftpproxytype="HttpConnect" httpproxybypasslocal="True"
        httpproxyusage="False" httpproxyauthentication="False" httpproxyusername="" httppr
        "" httpusestandardproxy="True" httpproxyport="3128" httpproxytype="HttpConnect" ft
        True" httpuri="http://127.0.0.1/" ftphost="" ftpfolder="/livezilla" id="localhost"
        ftpport="21" ftpanonymous="False" />
  </server>
</LiveZilla>
```

Mitigation

Administrators passwords should not be stored in files as plaintext. The 1click design should be changed so that as an example the 1click file asks the administrator for a password before opening. This way it can be assured that the administrator password is not disclosed to attackers.

3. Proof of Concept Codes:

Just open the xml based onclick file.

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 patched version
28.11.2013	Disclosed to public