GNet Solutions - Bug #139

Rooting a Samsung SCH-I500 Mesmerize US Cellular Android Smartphone the Hard Way

07/08/2013 02:26 PM - Daniel Curtis

Status:	Closed	**Start date:**	07/08/2013
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:		**Estimated time:**	3.00 hours
Target version:		**Spent time:**	7.00 hours

Description

During my attempts to directly root my recently acquired Samsung Mesmerize, I found that all attempts failed miserably. I used the following methods to try and obtain root:

1. SuperOneClick v2.3.3
2. z4root
3. zergRush automated linux script

However all of these methods failed to properly execute the exploit. This led me to replace the existing stock Samgsung ROM with the most current stable build of CyanogenMod 7.2. I had to enable USB debugging and push the file to the smartphones SD card.

Download CyanogenMod and push to smartphone

```
wget http://get.cm/get/95w
mv cm-7.2* update.zip
sudo adb kill-server
sudo adb start-server
adb push update.zip /sdcard/
```

Once this completed I attempted to put the device into recovery mode and apply an update from the SD card, this however resulted in an error stating the package was not signed. I needed a different recovery manager.

Installing Heimdall and flashing Clockwork Recovery

I downloaded Clockwork Recovery for the Mesmerize here but I have included a copy for posterity. Once I had Clockwork Recovery I needed to flash it to the smartphone using Heimdall, I have included two DEB packages to install Heimdall and Heimdall Frontend to install onto any Debian/Ubuntu system.

Install Heimdall

```
dpkg -i heimdall*
```

Flash Clockwork Recovery

```
tar xf cwm4-bml-i500.tar
heimdall flash --recovery recovery.bin --no-reboot
```

Install CyanogenMod from Clockwork Recovery

Once the upload completed I had to pull the battery to reboot the device. I held the **Vol. UP** and **Vol. DOWN** during boot to put the device into recovery mode.

1. Select the option to wipe data/factory reset.
2. Select install zip from sdcard
3. Select choose zip from sdcard
4. Select the CyanogenMod file you placed on the sdcard

You will then need to then confirm that you do wish to flash this file. Once completed the new ROM booted perfect. However Cyanogenmod does not include Google Apps, such as the Play Store, by default as Cyanogenmod takes an isolated approach. This means I needed to put the GApps on this device and was done by downloading the GApps provided by CyanogenMod; I have included a copy for archiving.

Upload and Install GApps via Clockwork Recovery

I bricked my new device numerous time during this process, one reason was due to mounting the system partition as read/write and tried to install the GApp while the system was running. This is a task better left to Clockwork Recovery.

```
adb push gapps-gb* /sdcard/
adb reboot
```

1. Hold **Vol. UP** and **Vol. DOWN** while powering on the device
2. Select install zip from sdcard
3. Select choose zip from sdcard
4. Select the CyanogenMod file you placed on the sdcard
5. Reboot the device

History

#1 - 07/09/2013 07:54 AM - Daniel Curtis

- Subject changed from Rooting a Samsung ICH-500 Mesmerize US Cellular Android Smartphone the Hard Way to Rooting a Samsung SCH-I500 Mesmerize US Cellular Android Smartphone the Hard Way

#2 - 11/27/2013 02:04 PM - Daniel Curtis

The heimdall package is available in Ubuntu repositories. It can be installed with the following command:

```
sudo apt-get install heimdall-flash heimdall-flash-frontend
```

Files

cwm4-bml-i500.tar	5.6 MB	07/08/2013	Daniel Curtis
heimdall_1.3.2_i386.deb	41.4 KB	07/08/2013	Daniel Curtis
heimdall-frontend_1.3.2_i386.deb	91.4 KB	07/08/2013	Daniel Curtis
gapps-gb-20110828-signed.zip	6.11 MB	07/08/2013	Daniel Curtis
cm-7.2.0-mesmerizemtd.zip	98.5 MB	07/08/2013	Daniel Curtis