

[NEWS] eSeSIX Thintune Thin Client Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0086.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/25/04

To: list@securiteam.com

Date: 25 Jul 2004 15:10:21 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

eSeSIX Thintune Thin Client Multiple Vulnerabilities

SUMMARY

<<http://www.thintune.com>> Thintune is "a series of thin client appliances sold by eSeSIX GmbH, Germany". They offer ICA, RDP, X11 and SSH support based on a customized Linux platform. Multiple security vulnerabilities have been found in the product allowing complete compromise of the system.

DETAILS

Affected Product:

All Linux-based Thintune models with firmware version 2.4.38 and prior

The following device was tested:

* Thintune M, Firmware version 2.4.38-32-D

* VIA Centaur processor (533 MHz), 128 MB RAM

Software version: JSTREAM II 2.4.38

According to the vendor, all Linux based Thintune models with firmware version up to (and including) v2.4.38 are affected. The vulnerabilities 1, 2, 3 and 4 are fixed in firmware version 2.4.39. eSeSIX claims that Windows CE based Thintune models are not vulnerable.

Securiteam: [NEWS] eSeSIX Thintune Thin Client Multiple Vulnerabilities

Vulnerabilities:

1. REMOTE ROOT SHELL / BACKDOOR

By connecting to an undocumented process on the Thintune over the network an attacker can gain full control over the thin client without notice by the local user. This includes running installed programs, transferring files to and from the network, powering down the system and updating the firmware.

Details:

There is an undocumented process listening on TCP port 25072 that can be given one of the following commands after authenticating by a short password. This password ("jstwo") is hardcoded into the /usr/bin/radmin shell script and cannot be changed via the configuration interface. [1]

shell – give root shell
version – show hardware version
beep – start beeping
restart – reboot immediately
poweroff – power off immediately
info – display pop-up message via xmsg
firmware – download firmware from given URL
getreg – get local configuration settings

Exploit:

```
$ nc 192.168.1.77 25702
JSRAFV-1
jstwo <- hardcoded password
+yep
shell <- one of several commands shown above
+yep here you are ...
id <- run "id" to show my privileges
uid=0(root) gid=0(root)
```

The Thintune firmware includes BusyBox v0.47 which gives you access to nc, dd, tar, mount, kill, powerdown and other utilities. In my case, there was about 4MB of free space on the flash card used as hard drive.

According to the vendor, this backdoor is used by the eSeSIX support team when the management software is not available at the customer site or is not working correctly.

[1] Of course you could change the hardcoded password after exploiting vulnerabilities #1 or #3 and gaining a root shell.

Recommended fix:

Upgrade to firmware version 2.4.39 or newer. (The backdoor stays in place but uses a challenge-response system for authentication)

Temporary workaround:

Open local root shell by exploiting vulnerability #3 (see below), edit /etc/inetd.conf and delete the line concerning port 25702. Reboot.

2. DETERMINE PASSWORDS REMOTELY

All configuration settings can be acquired remotely, including saved user names and passwords for RDP and ICA connections as well passwords for the local VNC server, the JStream control center and the screensaver.

Details:

The Keeper library [2] is used to store all JStream configuration settings. Configuration files are stored in the /root/.keeper/ directory. Every section of the database has its own subdirectory and every configuration setting is put into a file in that subdirectory.

[2] <<http://kempelen.iit.bme.hu/~mszeredi/keeper/keeper.html>>
<http://kempelen.iit.bme.hu/~mszeredi/keeper/keeper.html>

By browsing the local file system or (more comfortably) using the "getreg" command shown above, one can remotely read out this Keeper database. The following sections and keys may be particularly interesting for an attacker:

desktop shadow_password – VNC password (VNC is called "shadowing")
security adminpassword – control center (administrator) password
security userpassword – screen saver password

ica con_0_9 – username for first ICA connection
ica con_0_10 – password for first ICA connection
ica con_0_11 – domain for first ICA connection
ica con_0_3 – address for first ICA connection

rdp con_0_6 – username for first RDP connection
rdp con_0_7 – password for first RDP connection
rdp con_0_8 – domain for first RDP connection
rdp con_0_3 – address for first RDP connection

Connection settings and passwords for other protocols can be found in the rdppro, ssh, tarantella and rexec subdirectories in the same way.

All passwords are stored in clear text in the corresponding files.

Exploit:

```
$ nc 192.168.1.77 25702
JSRAFV-1
jstwo
+yep
getreg
+yep enter section and key
desktop shadow_password
myVNCpwd
```

Recommended fix:

Upgrade to firmware version 2.4.39 or newer.

Securiteam: [NEWS] eSeSIX Thintune Thin Client Multiple Vulnerabilities

Temporary workaround:

Open local root shell by exploiting vulnerability #3 (see below), edit `/etc/inetd.conf` and delete the line concerning port 25702. Reboot.

3. LOCAL ROOT SHELL

Any local user of the thin client can launch a local root shell by pressing some keys and entering a special password. Attackers could use this shell to acquire all passwords in the Keeper database (see above).

This feature has not been documented, but is shown to the customer during support sessions when needed.

Exploit:

Press `<CTRL><SHIFT><ALT>` and enter "maertsJ" as password. An xterm window is launched that runs with root privileges. The password is hardcoded into the `/usr/bin/lshell` executable and cannot be changed.

For an alternate attack vector, use the Phoenix web browser to open the file `/usr/bin/lshell` with itself (see below).

Recommended fix:

Upgrade to firmware version 2.4.39 or newer, which uses a challenge–response system for authentication.

Temporary workaround:

Delete `/usr/bin/lshell` (Be sure to apply workarounds for vulnerabilities 1 and 2 first).

4. VIEW CLEARTEXT PASSWORDS LOCALLY VIA WEB BROWSER

Any local user can browse the complete file system by using an existing web browser connection and entering a simple URL into the address bar. As the control center, screensaver and VNC passwords are stored in clear text files; a local attacker can read them.

Details:

The Thintune software supports WWW access for end users via the Phoenix web browser (now called Mozilla Firefox).

Entering "file:/// " into the Phoenix URL address bar shows the root directory of the local file system. As Phoenix is run with root privileges, there are no restrictions concerning the files that can be viewed.

Using this technique, clear text passwords can be found in several files. Some examples:

```
/root/.keeper/desktop/shadow_password – VNC  
/root/.keeper/desktop/security/adminpassword – control center  
/root/.keeper/security/userpassword – screen saver password  
/usr/bin/radmin – remote control (see Vuln.#1)
```

Securiteam: [NEWS] eSeSIX Thintune Thin Client Multiple Vulnerabilities

Note: Web browsing has to be enabled by the administrator in the JStream control center by creating a Web connection. Access to the JStream control center can be password protected. Nevertheless, by exploiting vulnerability 3 and viewing the configuration file a local attacker can easily determine this password and get access to the control center.

Recommended fix:

Upgrade to firmware version 2.4.39 or newer (The browser has been put into a sandbox.)

Temporary workaround:

Delete all Phoenix connections.

5. PROBLEMATIC PASSWORD CHECKING

When prompted for the control center and lshell passwords, you do not have to press <Enter> to complete your input. Authentication takes place as soon as you have given the right password. This could make password guessing much easier.

Example:

Password is "a". No matter if you try "automobile", "any" or "afternoon" — as soon as you press the first "a" you are authenticated.

Recommended fix:

No fix is available at the moment.

Temporary workaround:

Choose long passwords.

Method Used for Research

Try browsing the local file system via the "file:///"-URL. Further examination gives the following interesting details:

- * local configuration files are placed in /root/.keeper
- * Two files in /root/.keeper/security/ show the administrator and screensaver passwords in cleartext.
- * /usr/bin/radmin seems to be a shell script that offers remote control commands. Password is shown in cleartext.

Opening /usr/bin/lshell (local shell?) via the web browser gives password prompt. Password is not known at this point

- * /root/.icewm/keys shows that lshell can be run by pressing <CTRL><ALT><SHIFT>

Nmap portscan against Thintune shows open TCP port 25702 (among others). Connecting to this port gives the "JSRAFV-1" reply that was found in local file /usr/bin/radmin before.

Gain remote root shell by giving the password found in /usr/bin/radmin and transfer local file system over the network using dd and nc.

Securiteam: [NEWS] eSeSIX Thintune Thin Client Multiple Vulnerabilities

Viewing /usr/bin/lshell in hex-editor on remote system shows clear text password for local shell access.

Browsing the /root/.keeper/ directory shows all connection settings in clear text.

Playing with the "getreg" command reveals that all settings can be acquired remotely.

Disclosure Timeline:

2004-05-29 Vulnerabilities found by Dirk Loss

2004-06-02 Vendor notification per phone and E-Mail

2004-06-07 Vendor confirms vulnerabilities and promises fixing the problems in next firmware release

2004-07-16 New firmware v2.4.39 released including fixes for problems 1-4

2004-07-24 Public disclosure

ADDITIONAL INFORMATION

The information has been provided by <mailto:Dirk.Loss@it-consult.net>
Dirk Loss.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.