Date: Nov. 30, 2014
From: http://Communications.Support Forums
To: Motorola Solutions Inc. - MOTOTRBO Product Group

Subject: MOTOTRBO Restricted Access to System (RAS) security vulnerability

Models/System Affected:
ALL MOTOTRBO subscriber radios. XPR4000/6000 >R01.11.02, XPR5000/7000 >R02.06.02, including System Release R02.40.00 (Unknown if lower-tier radios are affected; not tested.) operating on repeaters running Restricted Access to System (RAS), in standalone or IP Site Connect (IPSC) mode. Repeaters are not affected by this fault.

Symptoms:
When subscriber equipment is operating on a stand-alone digital or IP Site Connect (IPSC) repeater and the repeater and subscriber equipment is configured to use the Restricted Access to System (RAS) feature, a malicious outside party who does not possess the RAS key is able to transmit on the output of the repeater (while idle) in simplex mode and:

- Send one-way Group Call voice transmissions to RAS-protected users (on selected talkgroup);
- Send radio-to-radio Call Alert queries to RAS-protected users;
- Send Radio Check queries to selected RAS-protected users;
- Send Radio Disable command to selected RAS-protected users;
- Send Radio Enable command to selected RAS-protected users;
- Send Text Message(s) to selected RAS-protected users;
- Send false Emergency Alarm or Emergency Call transmissions to selected RAS-protected users.

A malicious user is able to gather Radio IDs, Group Call IDs, repeater Color Code and Timeslot information by utilizing third-party software applications which monitor DMR transmissions. This logged information is then programmed into the malicious radio and used to harass users on the RAS-protected repeater/system.

Additionally, when the malicious user targets a RAS-enabled subscriber and sends Call Alert, Radio Check, Radio Disable/Enable and Text Message queries/message(s), the targeted subscriber radio replies (sends outbound confirmation packets) on the output of the repeater in simplex mode, regardless of whether or not the “Allow Talkaround” feature enabled in the subscriber codeplug. These confirmations are received and displayed to the operator of the malicious radio.

Cause:
Subscriber firmware defect. The subscriber Radio Operating System (ROS) is not checking if incoming signals (on simplex) are encoded with the proper RAS key before executing operations or unmuting to voice transmissions.

Resolution:
There is no resolution available.

Severity of fault:
Serious. A malicious outside entity can disable subscriber radios, send false messages, divert resources and cause life-safety concerns.