Mobile (in)Security - Bug #1477

RACH flood DoS

02/19/2016 10:51 PM - laforge

Status:	New	**Start date:**	
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Um (MS-BTS) interface		
Target version:			
Resolution:		**Spec Reference:**	

Description

On the RACH (part of the CCCH/BCCH), the number of RACH slots per unit of time is fixed. The maximum possible number of RACH slots with a single-timeslot CCCH is 200.

Furthermore, the number of available dedicated (control and traffic) channels is limited in any given cell.

As per the GSM specification, any newly-assigned dedicated channel has to stay assigned for 2 seconds, waiting for the MS to establish the radio link layer. Only after 2 seconds, the channel can be closed and re-used for other purposes.

If anyone can send more RACH requests (in 2 seconds) than the cell has dedicated channels, permanent resource exhaustion of dedicated channels will happen (in other words, a DoS).

As the RACH request can be hand-crafted by the attacker and sent at a timing chosen by the attacker, there is no possibility for the BTS to differentiate real from malicious RACH bursts.

This attack has been implemented in 2009 by Dieter Spaar, and has been publicly demonstrated at the Deepsec 2009 conference in Vienna.

Slides are available from http://www.mirider.com/GSM-DoS-Attack_Dieter_Spaar.pdf

History

#1 - 07/31/2010 09:14 AM - admin

- Status changed from New to Closed

- Resolution set to confirmed

#2 - 07/31/2010 09:15 AM - admin

- Status changed from Closed to Feedback

- Resolution deleted (confirmed)

#3 - 02/21/2016 04:34 PM - laforge

- Assignee deleted (laforge)