

DragonFlyBSD - Bug #3015

sbin/gpt/show.c:133: do we always find what we are looking for ?

04/11/2017 11:11 AM - dcb

Status:	New	Start date:	04/11/2017
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:			
Description			
dragonfly/sbin/gpt/show.c:133]: (error) Array 'mbr.mbr_part[4]' accessed at index 4, which is out of bounds.			
Source code is			
<pre>for (i = 0; i < 4; i++) { start = le16toh(mbr->mbr_part[i].part_start_hi); start = (start << 16) + le16toh(mbr->mbr_part[i].part_start_lo); if (m->map_start == p->map_start + start) break; } printf("%d", mbr->mbr_part[i].part_typ);</pre>			
In the final printf, the code assumes we have found what we are looking for.			
Maybe the code would be stronger if it dealt with the case where it didn't.			