Description
The B2GM MPM matcher has questionable code related to use of B2gmPattern1 structures. These are only used for patterns of length 1.

The array ctx->patterns1 is of type uint8_t*, but are then always cast to B2gmPattern1 pointers. Why is patterns1 not of type (B2gmPattern1*)?
Offsets into the uint8_t array are started at 1 with a comment about skipping the first byte of the buffer. This will always result in unaligned access to the structure.

History
#1 - 09/30/2014 03:57 AM - Victor Julien
Probably not worth fixing, instead we can remove this code. Don't think anyone uses it.

#2 - 09/30/2014 08:56 AM - Ken Steele
My work around was to remove the b2gm and b2gc MPM.

#3 - 02/16/2016 04:20 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

Do we have some updates for that? :)

#4 - 02/17/2016 02:07 AM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Victor Julien
- Target version changed from TBD to 3.1

Scheduled for removal in 3.1.

#5 - 04/04/2016 10:44 AM - Victor Julien
- Target version changed from 3.1 to 3.1rc1

#6 - 04/05/2016 04:20 AM - Victor Julien
- Status changed from Assigned to Closed

https://github.com/inliniac/suricata/pull/1980