icmpv4 error packets can lead to missed detection in tcp/udp

08/31/2016 02:05 AM - Victor Julien

Description
If an ICMPv4 error packet is received as the first packet on a flow in the to_client direction, it confuses the rule grouping lookup logic. The toclient inspection will then continue with the wrong rule group. This can lead to missed detection.

History
#1 - 09/01/2016 01:42 AM - Victor Julien
- Status changed from Assigned to Closed

https://github.com/inliniac/suricata/pull/2210

#2 - 09/01/2020 10:44 AM - Victor Julien
- Tracker changed from Bug to Security
- CVE set to 2016-10728
- Git IDs updated