With the adoption of cloud computing, horizontally scalable infrastructure, and containerized deployments, Software Defined Networking (SDN) became an integral part of data centers, Kubernetes and Open vSwitch (OVS) being one of the commonly deployed solutions. Our work explores the possible performance limitations of OVS under Kubernetes, focusing on pathological traffic patterns. We discovered several types of packets causing excess system load on the cluster nodes. We identified the root cause as a series of drop rules in OpenFlow and a design flaw in OVS that prevents their efficient evaluation. We investigated the impact of this problem and our research revealed a specific system configurations under which an adversary can use the discovered inefficiencies for a practical denial of service attack on the local cluster node, bringing the whole networking stack down for all neighbouring containers.