```
Message-ID: <nycvar.YSQ.7.76.1810081020570.6766@xnncv>
Date: Mon, 8 Oct 2018 10:35:19 +0530 (IST)
From: P J P <ppandit@...hat.com>
To: oss security list <oss-security@...ts.openwall.com>
cc: Arash TC <tohidi.arash@...il.com>, Daniel Shapira <daniel@...stlock.com>
Subject: Qemu: integer overflow issues

   Hello,

Multiple integer overflow issues were found and reported in various NIC
emulations in QEMU. These integer overflow could occur while receiving packets
and could lead to OOB stack buffer access, resulting in DoS scenario.


* CVE-2018-10839 Qemu: ne2000: integer overflow leads to buffer overflow issue

Upstream fix:
   -> https://lists.gnu.org/archive/html/qemu-devel/2018-09/msg03273.html

* CVE-2018-17958 Qemu: rtl8139: integer overflow leads to buffer overflow

Upstream fix:
   -> https://lists.gnu.org/archive/html/qemu-devel/2018-09/msg03269.html

* CVE-2018-17962 Qemu: pcnet: integer overflow leads to buffer overflow

Upstream fix:
   -> https://lists.gnu.org/archive/html/qemu-devel/2018-09/msg03268.html

* CVE-2018-17963 Qemu: net: ignore packets with large size

Upstream fix:
   -> https://lists.gnu.org/archive/html/qemu-devel/2018-09/msg03267.html


These issues were independently reported by Arash TC and Daniel Shapira.


Thank you.
--
Prasad J Pandit / Red Hat Product Security Team
47AF CE69 3A90 54AA 9045 1053 DD13 3D32 FE5B 041F
```