Issues

One strange issue I found so far is in Frame 3

Frame number...3...

Eth:  \*\*\*\*\*\*\* Ethernet - "Ethernet" - offset=0 (0x0) length=14 protocol suite=LAN

Eth:

Eth:                              destination = 90:e2:ba:89:3c:53

Eth:                    .... ..0. .... .... = [2] LG bit

Eth:                    .... ...0 .... .... = [0] IG bit

Eth:                                   source = 00:10:18:65:4b:53

Eth:                    .... ..0. .... .... = [2] LG bit

Eth:                    .... ...0 .... .... = [0] IG bit

Eth:                                     type = 0x806 (2054)

Eth: 033602[B@3796751b[B@67b64c4502[B@3796751b[B@67b64c45

its an ARP message and yet destination is a specific address not [ff:ff:ff:ff:ff:ff]

I thought always destination in ARP should be like that [ broadcasting ]

so address 00:10:18:65:4b:53 in Frame 2 sent a normal ARP, but some how strange ARP in Frame 3

This is Frame 2

Frame number...2...

Eth:  \*\*\*\*\*\*\* Ethernet - "Ethernet" - offset=0 (0x0) length=14 protocol suite=LAN

Eth:

Eth:                              destination = ff:ff:ff:ff:ff:ff

Eth:                    .... ..0. .... .... = [2] LG bit

Eth:                    .... ...0 .... .... = [2] IG bit

Eth:                                   source = 90:e2:ba:89:3c:53

Eth:                    .... ..0. .... .... = [2] LG bit

Eth:                    .... ...0 .... .... = [2] IG bit

Eth:                                     type = 0x806 (2054)

Eth: 048022[B@71be98f5[B@6fadae5d22[B@71be98f5[B@6fadae5d

Frame number...1... ... not a TCP packet

Frame number...2... ... not a TCP packet

Frame number...3... ... not a TCP packet

Frame number...4...<192.168.1.2,48684> ==> <192.168.1.1,6633> first SYN, ISN=42347239

Frame number...5...<192.168.1.1,6633> ==> <192.168.1.2,48684> SYN/ACK, ISN=1740973611

ISNs should match

1) A --> B SYN my sequence number is X

2) A <-- B ACK your sequence number is X

3) A <-- B SYN my sequence number is Y

4) A --> B ACK your sequence number is Y

---------------------------------\

Usually response ISN sequence number should be the sent one plus one [ which is not the case above ]

Frame number...4...<192.168.1.2,48684> ==> <192.168.1.1,6633> first SYN, ISN=42347239

Frame number...5...<192.168.1.1,6633> ==> <192.168.1.2,48684> SYN/ACK, ISN=1740973611

--------------------- a known vulnerability

<https://www.cvedetails.com/vulnerability-list/vendor_id-12098/Openvswitch.html>

# [Openvswitch](https://www.cvedetails.com/vendor/12098/Openvswitch.html) : Security Vulnerabilities

CVSS Scores Greater Than: [0](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)   [1](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=1&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)   [2](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=2&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)   [3](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=3&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)   [4](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=4&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)   [5](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=5&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)   [6](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=6&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)   [7](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=7&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)   [8](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=8&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)   [9](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=9&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)

Sort Results By : [CVE Number Descending](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)   [CVE Number Ascending](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&month=0&cweid=0&order=2&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)   [CVSS Score Descending](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&month=0&cweid=0&order=3&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)   [Number Of Exploits Descending](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&month=0&cweid=0&order=4&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7)

[Copy Results](javascript:sertabletotsv('vulnslisttable',true,false,'downloadoverlaydivtxtarea')) [Download Results](javascript:sertabletotsv('vulnslisttable',true,true,null)) [Select Table](javascript:selectdiv('searchresults'))

Top of Form

Bottom of Form

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **#** | **CVE ID** | **CWE ID** | **# of Exploits** | **Vulnerability Type(s)** | **Publish Date** | **Update Date** | **Score** | **Gained Access Level** | **Access** | **Complexity** | **Authentication** | **Conf.** | **Integ.** | **Avail.** |
| 1 | [CVE-2012-3449](https://www.cvedetails.com/cve/CVE-2012-3449/) | [264](https://www.cvedetails.com/cwe-details/264/cwe.html) |  |  | 2012-08-07 | 2012-08-08 | **3.6** | None | Local | Low | Not required | None | Partial | Partial |
| Open vSwitch 1.4.2 uses world writable permissions for (1) /var/lib/openvswitch/pki/controllerca/incoming/ and (2) /var/lib/openvswitch/pki/switchca/incoming/, which allows local users to delete and overwrite arbitrary files. | | | | | | | | | | | | | | |

Total number of vulnerabilities : **1**   Page : [1](https://www.cvedetails.com/vulnerability-list.php?vendor_id=12098&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=1&sha=2b521c29ec4796232c5b6ee79993e646c153f7a7) (This Page)

------------------------