Hi Zhang Li & Hua Bin,

十分感谢关于此问题的分析，这个案例可以关闭了。

贾伟 Jia Wei
神州网信技术有限公司
服务电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Bin Hua <bihua@microsoft.com>
发送时间: 2020 年 10 月 12 日 17:47
收件人: Li Zhang <zhaling@microsoft.com>; Jia Wei <jiawei@cmgos.com>
抄送: Li Xin <lixin@cmgos.com>; Tony Ma (CSAM) <yima@microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; support <support@mail.support.microsoft.com>
主题: RE: 120101226001556 CAS-02966-Z6Y0H0 - 珠海二部领导蓝屏

Hi 贾伟

以下是 vwifimf 的 filter 信息：

```
0: kd> !ndiskd.filterdriver ffffb78447e94d50


FILTER DRIVER

    NDIS Sample LightWeight Filter 1

    Ndis handle         ffffb78447e94d50    dt  ffffb78447e94d50
ndis!_NDIS_FILTER_DRIVER_BLOCK
    Driver context      ffffb7844c2acde0
    Ndis API version    v6.0
    Driver version      v1.0
    Driver object       ffffb7844c2acde0
    Driver image        vwifimf.sys

    Bind flags          Mandatory, Modifying, UnbindOnAttach, UnbindOnDetach
    Class               ms_medium_converter_128
    References          2
```

FILTER MODULES

Filter module	
ffffb784509ccb20	Intel(R) Wireless-AC 9560 160MHz-NDIS Sample LightWeight Filter 1-0000

HANDLERS

Filter handler	Function pointer	Symbol (if available)
SetOptionsHandler	fffff80124cc1720	vwifimf+1720
SetFilterModuleOptionsHandler	fffff80124cc249c	vwifimf+249c
AttachHandler	fffff80124cc1744	vwifimf+1744
DetachHandler	fffff80124cc1aa4	vwifimf+1aa4
RestartHandler	fffff80124cc1a14	vwifimf+1a14
PauseHandler	fffff80124cc19c4	vwifimf+19c4
SendNetBufferListsHandler	fffff80124cc1fb4	vwifimf+1fb4
SendNetBufferListsCompleteHandler	fffff80124cc1e28	vwifimf+1e28
CancelSendNetBufferListsHandler	fffff80124cc2488	vwifimf+2488
ReceiveNetBufferListsHandler	fffff80124cc2214	vwifimf+2214
ReturnNetBufferListsHandler	fffff80124cc2184	vwifimf+2184
OidRequestHandler	fffff80124cc1bc4	vwifimf+1bc4
OidRequestCompleteHandler	fffff80124cc1d00	vwifimf+1d00
DirectOidRequestHandler	[None]	
DirectOidRequestCompleteHandler	[None]	
SynchronousOidRequestHandler	[None]	
SynchronousOidRequestCompleteHandler	[None]	
CancelDirectOidRequestHandler	[None]	
DevicePnPEventNotifyHandler	fffff80124cc1e00	vwifimf+1e00
NetPnPEventHandler	fffff80124cc1e14	vwifimf+1e14
StatusHandler	fffff80124cc1dec	vwifimf+1dec

华斌
Support Escalation Eng | Microsoft China Co Ltd | +86 (510) 66657739 | bihua@microsoft.com

---

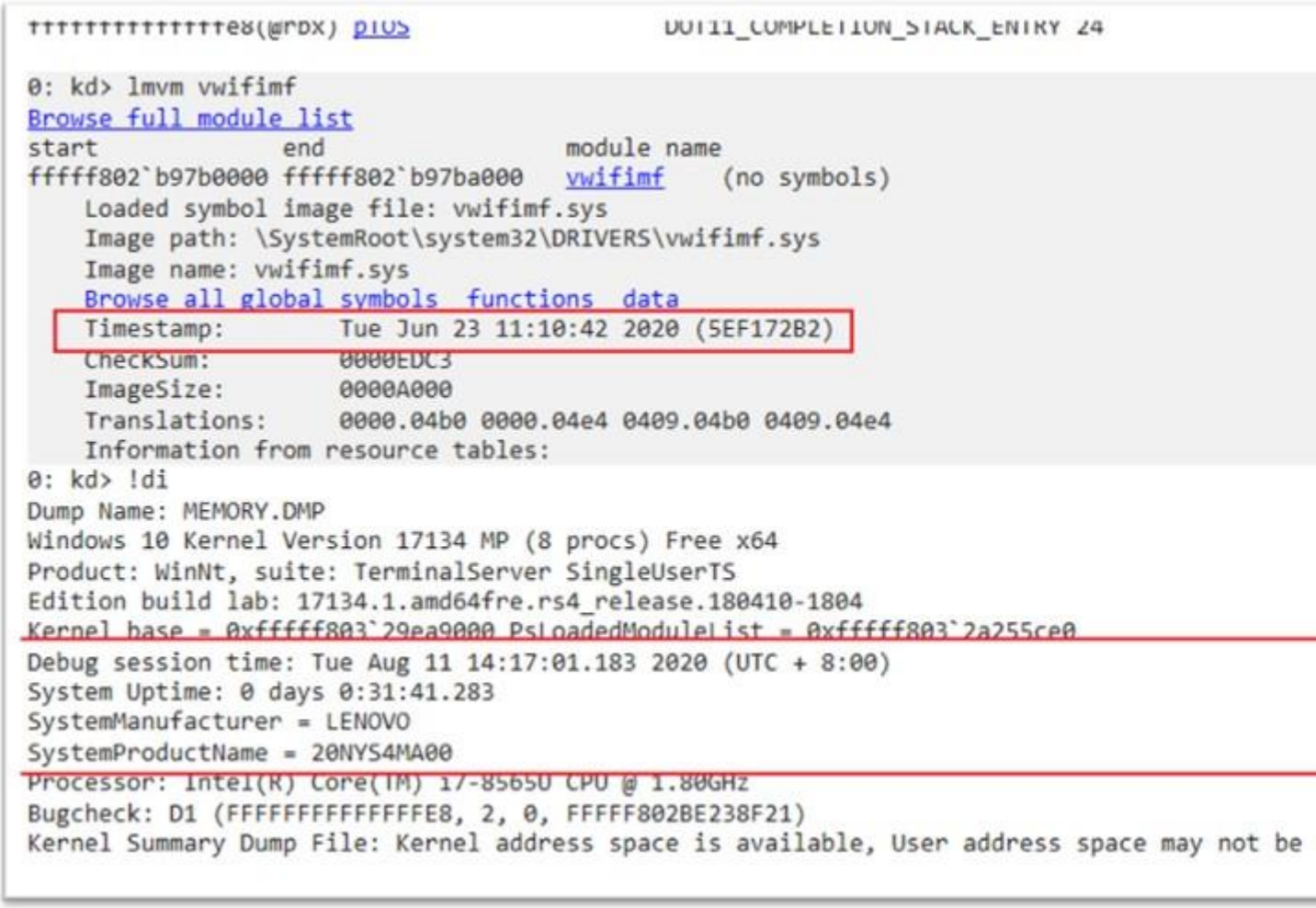
From: Bin Hua
Sent: 2020 年 10 月 12 日 16:39
To: Li Zhang <zhaling@microsoft.com>; jiawei@cmgos.com
Cc: lixin@cmgos.com; Tony Ma (CSAM) <yima@microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; support <support@mail.support.microsoft.com>
Subject: RE: 120101226001556 CAS-02966-Z6Y0H0 - 珠海二部领导蓝屏

Hi 贾伟，您好

今天收集的版本的蓝屏已分析完毕，原因和之前 vwifimf 的系列案件是一样的。Call stack 有区别是由于网卡驱动版本的不同。之前比较多的网卡驱动是 netwtw06，而本 dump 的网卡驱动是 netwtw08。

其实之前（8 月 17 日）我们也收集到并分析过 netwtw08 驱动的 dump，见附件邮件。

另外，对比 vwifimf 的版本，8 月 17 日的 dump 和今天的 dump 版本应该是一样的。



Dump 分析:

```
0: kd> .frame 0n3;dv /t /v
03 fffff801`21e78d40 fffff801`29ffd66d     nwifi!Dot11SendCompletion+0x35
[onecoreuap\net\wlan\sys\infra\driver\pktutil.c @ 100]
@rsi               struct _NET_BUFFER_LIST * pNdisPacket = 0xffffb784`58ad6350
 _NET_BUFFER_LIST
@ebp               int ndisStatus = 0n0
@rdi               struct DOT11_COMPLETION_STACK_ENTRY * pBOS = 0xffffb784`51ef6b00
@rbx               struct DOT11_COMPLETION_STACK_ENTRY * pTOS = 0xffffffff`fffffff8

0: kd> dt ffffb78458ad6350 DOT11_PACKET
nwifi!DOT11_PACKET
 _NET_BUFFER_LIST
   +0x000 Next             : (null)
   +0x008 FirstNetBuffer   : 0xffffb784`58ad64d0  _NET_BUFFER
   +0x000 Link             : _SLIST_HEADER
   +0x000 NetBufferListHeader : _NET_BUFFER_LIST_HEADER
   +0x010 Context          : 0xffffb784`51ef6ac0 _NET_BUFFER_LIST_CONTEXT
```

```
   +0x018 ParentNetBufferList : (null)
   +0x020 NdisPoolHandle   : 0xffffb784`509d0040 Void
   +0x030 NdisReserved     : [2] (null)
   +0x040 ProtocolReserved : [4] 0xffffb784`58aaf9c0 Void
   +0x060 MiniportReserved : [2] (null)
   +0x070 Scratch          : (null)
   +0x078 SourceHandle     : 0xffffb784`509ccb20 Void
   +0x080 NblFlags         : 0
   +0x084 ChildRefCount    : 0n0
   +0x088 Flags            : 0x500
   +0x08c Status           : 0n0
   +0x08c NdisReserved2    : 0
   +0x090 NetBufferListInfo : [26] (null)

0: kd> !pool 0xffffb784`51ef6ac0
Pool page ffffb78451ef6ac0 region is Nonpaged pool
 ffffb78451ef6000 size:   30 previous size:    0  (Allocated)  FSfc
 ffffb78451ef6030 size:   30 previous size:    0  (Allocated)  FSfc
 ffffb78451ef6060 size:   30 previous size:    0  (Allocated)  FOCX
 ffffb78451ef6090 size:   30 previous size:    0  (Allocated)  IoUs
 ffffb78451ef60c0 size:   30 previous size:    0  (Allocated)  FOCX
 ffffb78451ef60f0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6120 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6150 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6180 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef61b0 size:   30 previous size:    0  (Allocated)  FSfc
 ffffb78451ef61e0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6210 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6240 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6270 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef62a0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef62d0 size:   30 previous size:    0  (Allocated)  Io
 ffffb78451ef6300 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6330 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6360 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6390 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef63c0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef63f0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6420 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6450 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6480 size:   30 previous size:    0  (Allocated)  Io
 ffffb78451ef64b0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef64e0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6510 size:   30 previous size:    0  (Allocated)  FOCX
 ffffb78451ef6540 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6570 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef65a0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef65d0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6600 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6630 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6660 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6690 size:   30 previous size:    0  (Allocated)  FOCX
 ffffb78451ef66c0 size:   30 previous size:    0  (Allocated)  Ipcr
 ffffb78451ef66f0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6720 size:   30 previous size:    0  (Allocated)  Filt
```

```
 ffffb78451ef6750 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6780 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef67b0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef67e0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6810 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6840 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6870 size:   30 previous size:    0  (Allocated)  NDFL
 ffffb78451ef68a0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef68d0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6900 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6930 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6960 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6990 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef69c0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef69f0 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6a20 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6a50 size:   30 previous size:    0  (Allocated)  Filt
 ffffb78451ef6a80 size:   30 previous size:    0  (Allocated)  Filt
*ffffb78451ef6ab0 size:   30 previous size:    0  (Allocated) *Filt


0: kd> !tag Filt
Name    Number of Hits Version Time Stamp          Location
======= ============== ======= ==================
=======================================
vwifimf              1 0.0.0.0 06/23/2020 03:10:42
\SystemRoot\system32\DRIVERS\vwifimf.sys

Hits
============================================
fffff801`24cc1790  41 b8 46 69 6c 74 03 d1-0f b7 08 8d 94 0a 08 01  A.Filt.........
```

华斌
Support Escalation Eng | Microsoft China Co Ltd | +86 (510) 66657739 | bihua@microsoft.com

---

From: Li Zhang <zhaling@microsoft.com>
Sent: 2020 年 10 月 12 日 15:59
To: jiawei@cmgos.com
Cc: lixin@cmgos.com; Tony Ma (CSAM) <yima@microsoft.com>; Wxepscov <Wxepscov@microsoft.com>; Bin Hua <bihua@microsoft.com>; support <support@mail.support.microsoft.com>
Subject: RE: 120101226001556 CAS-02966-Z6Y0H0 - 珠海二部领导蓝屏

Loop Bin

From: Li Zhang <zhaling@microsoft.com>
Sent: 2020 年 10 月 12 日 13:48
To: jiawei@cmgos.com
Cc: lixin@cmgos.com; Tony Ma (CSAM) <yima@microsoft.com>; Li Zhang <zhaling@microsoft.com>;

Wxepscov <Wxepscov@microsoft.com>
Subject: 120101226001556 CAS-02966-Z6Y0H0 - 珠海二部领导蓝屏

贾先生， 您好!

感谢您联系微软全球技术中心。 我是微软的技术支持工程师 Li Zhang。 很高兴能有机会协助您解决该问题。 您可随时通过以下联系方式以及该问题事件号码 120101226001556 与我联系。

请把 dump 上传至如下的工作空间:

==========

File Transfer - Case 120101226001556

jiawei@cmgos.com

lixin@cmgos.com

谢谢!