

吴先生，您好！

很高兴收到您的邮件回复，根据回复的结果，我将暂时归档此问题。**案例归档后您会收到调查问卷的邮件，希望可以对我们的服务进行评价。**

工单的归档并不会影响我们为您提供技术支持服务，如果您的问题复现，或有新的问题出现，您也可以致电我们的技术支持热线 4008180055。

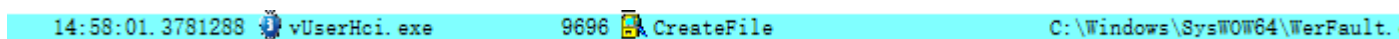
### 案例总结：

### 案例描述：

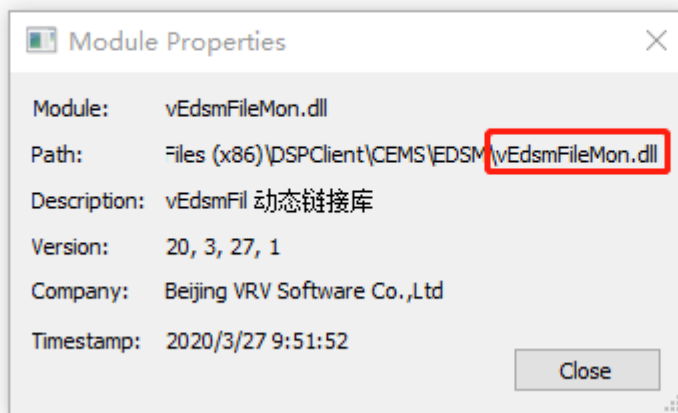
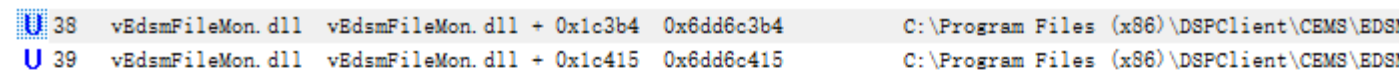
8 月补丁安装失败，在安装失败过程中弹出 vuser.exe 该进程为我行 DSP 加密文档的登陆程序。请从系统层面进行分析，8 月补丁更新哪些内容。

### 案例分析：

- 报错出现在 14:58:01 path:C:\Windows\SysWOW64\WerFault.exe 而触发的是 vUserHci.exe



- 在堆栈信息中看到 C:\Program Files (x86)\DSPClient\CEMS\EDSM\vEdsmFileMon.dll 引入，这个 vEdsmFileMon.dll 就很可疑



- 再根据最新提供的由 DSP 软件生产的 4 个 Minidump 文件，亦可以直接看到导致 Crash 问题与 vEdsmFileMon 模块有关。

SYMBOL\_NAME: vEdsmFileMon+1c415  
FOLLOWUP\_NAME: MachineOwner  
MODULE\_NAME: vEdsmFileMon  
IMAGE\_NAME: vEdsmFileMon.dll  
DEBUG\_FLR\_IMAGE\_TIMESTAMP: 5e7d5c38  
STACK\_COMMAND: ~14s ; .ecxr ; kb  
BUCKET\_ID: INVALID\_CRUNTIME\_PARAMETER\_vEd:  
FAILURE\_EXCEPTION\_CODE: c0000417  
FAILURE\_IMAGE\_NAME: vEdsmFileMon.dll  
BUCKET\_ID\_IMAGE\_STR: vEdsmFileMon.dll  
FAILURE\_MODULE\_NAME: vEdsmFileMon  
BUCKET\_ID\_MODULE\_STR: vEdsmFileMon  
FAILURE\_FUNCTION\_NAME: Unknown  
BUCKET\_ID\_FUNCTION\_STR: Unknown

Browse full module list

start end module name

6db00000 6db48000 vEdsmFileMon T (no symbols)

Loaded symbol image file: vEdsmFileMon.dll

Image path: C:\Program Files (x86)\DSPClient\CEMS\EDSM\vEdsmFileMon.dll

Image name: vEdsmFileMon.dll

Browse all global symbols functions data

Timestamp: Fri Mar 27 01:51:52 2020 (5E7D5C38)

Checksum: 00046D2E

ImageSize: 00048000

File version: 20.3.27.1

Product version: 1.0.0.1

File flags: 0 (Mask 17)

File OS: 4 Unknown Win32

File type: 2.0 Dll

File date: 00000000.00000000

Translations: 0000.04b0 0000.04e4 0409.04b0 0409.04e4

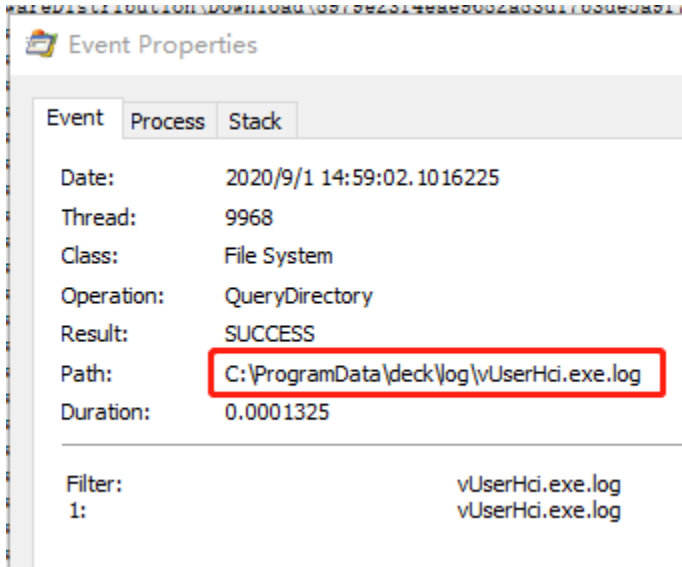
Information from resource tables:

建议操作:

1) vUserHci.exe 厂商进行进一步说明 vUserHci.exe 的功能和大量 NotfiyChangeDirectory 条目的具体行为。并重点排查 C:\Program Files (x86)\DSPClient\CEMS\EDSM\vEdsmFileMon.dll 文件的行为。

2) 如果针对 C:\全盘进行文件检测或保护等行为, 是否可以先将 C:\Windows\servicing\InboxFodMetadataCache、C:\Windows\servicing\InboxFodMetadataCache\metadata、和 C:\Windows\SoftwareDistribution\Download 文件夹加入例外, 尝试问题是否复现。如果问题不再复现, 可以逐一扩大定位位置。

3) Log 中发现 vUserHci.exe 会写 Log, 所以请 vUserHci.exe 厂商查看 C:\ProgramData\deck\log\vUserHci.exe.log 里关于此报错的记录。



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](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

发件人: [win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn) <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

发送时间: 2020 年 9 月 17 日 17:08

收件人: Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>

抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>; Liu Wei <[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>; Qi Feng <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>; Wang Dan <[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>; Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>

主题: 答复: 回复: 回复: [案例号: CAS-02878-F9R9D5 ] % |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应 CMIT:0001892

贾工，辛苦了。问题已经提交北信源公司解决。咱们这边可以归档了

发件人: "Jia Wei" <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>

收件人: "[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)" <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

抄送: "CRM Case Email" <[casemail@cmgos.com](mailto:casemail@cmgos.com)>, "Liu Wei" <[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>, "Qi Feng" <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>, "Wang Dan" <[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>, "Wang Wenlei" <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>

日期: 2020/09/17 16:40

主题: 回复: 回复: [案例号: CAS-02878-F9R9D5] % |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应 CMIT:0001892

吴先生，您好！

还未收到您的反馈。此案例的相关案例分析已经发送，可以查阅“2020 年 9 月 10 日 15:56”的内容。如果您对此有任何疑问，我很愿意为您解答。

-----  
-----  
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](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

发件人: Jia Wei

发送时间: 2020 年 9 月 15 日 14:32

收件人: 'win10sup@sdicbc.com.cn' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>; Liu Wei <[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>; Qi Feng <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>; Wang Dan <[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>; Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>

主题: 回复: 回复: [案例号: CAS-02878-F9R9D5 ] % |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应 CMIT:0001892

吴先生, 您好!

关于此问题是否有疑问或更新, 可以回复此邮件。

---

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](mailto:jiawei@cmgos.com)

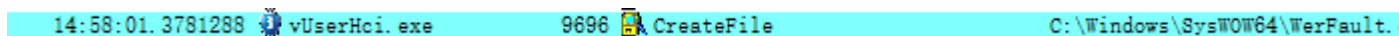
C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

发件人: Jia Wei  
发送时间: 2020 年 9 月 10 日 15:56  
收件人: 'win10sup@sdicbc.com.cn' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>  
抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>; Liu Wei <[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>; Qi Feng <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>; Wang Dan <[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>; Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>  
主题: 回复: 回复: [案例号: CAS-02878-F9R9D5 ] % |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应 CMIT:0001892

吴先生, 您好!

### 案例分析:

- 报错出现在 14:58:01 path:C:\Windows\SysWOW64\WerFault.exe 而触发的是 vUserHci.exe



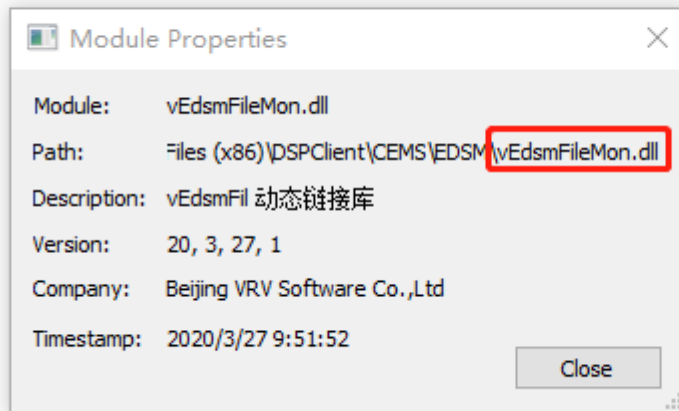
The screenshot shows a Windows Task Manager window with a cyan header bar. It displays the process 'vUserHci.exe' with PID 9696. The 'File' column shows it is performing a 'CreateFile' operation on 'C:\Windows\SysWOW64\WerFault.exe'.

- 在堆栈信息中看到 C:\Program Files (x86)\DSPClient\CEMS\EDSM\vEdsmFileMon.dll 引入, 这个 vEdsmFileMon.dll 就很可疑

```

U 38 vEdsmFileMon.dll vEdsmFileMon.dll + 0x1c3b4 0x6dd6c3b4 C:\Program Files (x86)\DSPClient\CEMS\EDSM
U 39 vEdsmFileMon.dll vEdsmFileMon.dll + 0x1c415 0x6dd6c415 C:\Program Files (x86)\DSPClient\CEMS\EDSM

```



- 再根据最新提供的由 DSP 软件生产的 4 个 Minidump 文件，亦可以直接看到导致 Crash 问题与 vEdsmFileMon 模块有关。

```

SYMBOL_NAME: vEdsmFileMon+1c415
FOLLOWUP_NAME: MachineOwner
MODULE_NAME: vEdsmFileMon
IMAGE_NAME: vEdsmFileMon.dll
DEBUG_FLR_IMAGE_TIMESTAMP: 5e7d5c38
STACK_COMMAND: ~14s ; .ecxr ; kb
BUCKET_ID: INVALID_CRUNTIME_PARAMETER_vEd:
FAILURE_EXCEPTION_CODE: c00000417
FAILURE_IMAGE_NAME: vEdsmFileMon.dll
BUCKET_ID_IMAGE_STR: vEdsmFileMon.dll
FAILURE_MODULE_NAME: vEdsmFileMon
BUCKET_ID_MODULE_STR: vEdsmFileMon
FAILURE_FUNCTION_NAME: Unknown
BUCKET_ID_FUNCTION_STR: Unknown

```

Browse full module list

start end module name

6db00000 6db48000 vEdsmFileMon T (no symbols)

Loaded symbol image file: vEdsmFileMon.dll

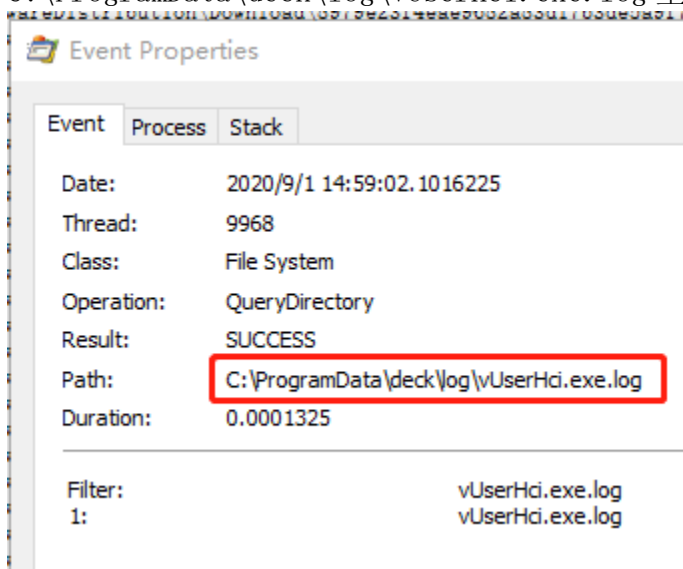
Image path: C:\Program Files (x86)\DSPClient\CEMS\EDSM\vEdsmFileMon.dll

Image name: vEdsmFileMon.dll

Browse all global symbols functions data  
Timestamp: Fri Mar 27 01:51:52 2020 (5E7D5C38)  
Checksum: 00046D2E  
ImageSize: 00048000  
File version: 20.3.27.1  
Product version: 1.0.0.1  
File flags: 0 (Mask 17)  
File OS: 4 Unknown Win32  
File type: 2.0 Dll  
File date: 00000000.00000000  
Translations: 0000.04b0 0000.04e4 0409.04b0 0409.04e4  
Information from resource tables:

### 建议操作:

- 1) vUserHci.exe 厂商进行进一步说明 vUserHci.exe 的功能和大量 NotfiyChangeDirectory 条目的具体行为。并重点排查 C:\Program Files (x86)\DSPClient\CEMS\EDSM\vEdsmFileMon.dll 文件的行为。
- 2) 如果针对 C:\全盘进行文件检测或保护等行为, 是否可以先将 C:\Windows\servicing\InboxFodMetadataCache、C:\Windows\servicing\InboxFodMetadataCache\metadata、和 C:\Windows\SoftwareDistribution\Download 文件夹加入例外, 尝试问题是否复现。如果问题不再复现, 可以逐一扩大定位位置。
- 3) Log 中发现 vUserHci.exe 会写 Log, 所以请 vUserHci.exe 厂商查看 C:\ProgramData\deck\log\vUserHci.exe.log 里关于此报错的记录。



\*上封邮件有关于 8 月累计更新变更的相关文件信息。

-----  
-----  
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](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

发件人: [win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn) <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>  
发送时间: 2020 年 9 月 10 日 14:56  
收件人: Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>  
抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>; Liu Wei <[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>; Qi Feng <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>; Wang Dan <[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>; Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>  
主题: 答复: 回复: [案例号: CAS-02878-F9R9D5 ] % |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应 CMIT:0001892

8 月份 V2020-L 累计更新补丁 KB4565349 安装问题现象如下:

- 1、TMS 文件监控策略限制了 wpdmtp.dll 时, 补丁安装失败
- 2、当 TMS 文件监控策略限制 wpdmtp.dll 并对 TiWorker.exe 进程进行例外时, 补丁可以成功安装, 但在安装过程中 DSP 会弹框 vUserHci.exe 报错并重启进程。

附件是替换 DSP 客户端文件后进行重新安装过程中产生的 dump 文件

发件人: Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>  
收件人: "[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)" <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>  
抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>, Liu Wei <[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>, Qi Feng <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>, Wang Dan <[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>, Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>  
日期: 2020/09/10 10:43  
主题: 回复: [案例号: CAS-02878-F9R9D5 ] % |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应 CMIT:0001892

---



吴先生，您好！

刚刚和案例联系人：侯佳俊先生电话沟通，关于此案例如果还需要其他信息或支持，您可以邮件回复。

经过查找相关资料，我又找到了关于 8 月份 V2020-L 累计更新补丁 KB4565349，和 V0-H 1020 累计更新补丁 KB4571709 中所提供的文件列表信息。

具体关于补丁安装的文件相关详细信息，如附件所示。

---

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](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

发件人: Jia Wei

发送时间: 2020 年 9 月 8 日 10:34

收件人: 'win10sup@sdicbc.com.cn' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>; Liu Wei <[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>; Qi Feng <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>; Wang Dan <[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>; Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>

主题: 回复: [案例号: CAS-02878-F9R9D5 ] % |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应 CMIT:0001892

吴先生，您好！

上周已经和案例联系人：侯佳俊先生电话沟通，关于此案例如果还需要其他信息或支持，您可以邮件回复。

---

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](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

发件人: Jia Wei  
发送时间: 2020 年 9 月 4 日 9:56  
收件人: 'win10sup@sdicbc.com.cn' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>  
抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>; Liu Wei <[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>; Qi Feng <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>; Wang Dan <[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>; Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>  
主题: 回复: [案例号: CAS-02878-F9R9D5 ]% |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应 CMIT:0001892

吴先生，您好！

经过查找相关资料，找到了关于 8 月份 V2020-L 累计更新补丁 KB4565349，和 V0-H 1020 累计更新补丁 KB4571709 中所提供的文件列表信息。  
具体关于补丁安装的文件相关详细信息，如附件所示。

-----  
-----  
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](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

发件人: Jia Wei  
发送时间: 2020 年 9 月 2 日 15:18  
收件人: 'win10sup@sdicbc.com.cn' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>  
抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>; Liu Wei <[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>; Qi Feng <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>; Wang Dan <[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>; Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>  
主题: 回复: [案例号: CAS-02878-F9R9D5 ]% |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应 CMIT:0001892

吴先生，您好！

问题定义：8月补丁安装失败，在安装失败过程中弹出 vuser.exe 该进程为我行 DSP 加密文档的登陆程序。请从系统层面进行分析，8月补丁更新哪些内容。

问题范围：协助您分析并处理上述问题。

接下来，我们将开始合作解决这个问题。如果您对以上的问题范围界定有任何异议，请尽快告知。如果您有其他任何疑问。也欢迎随时与我联系。

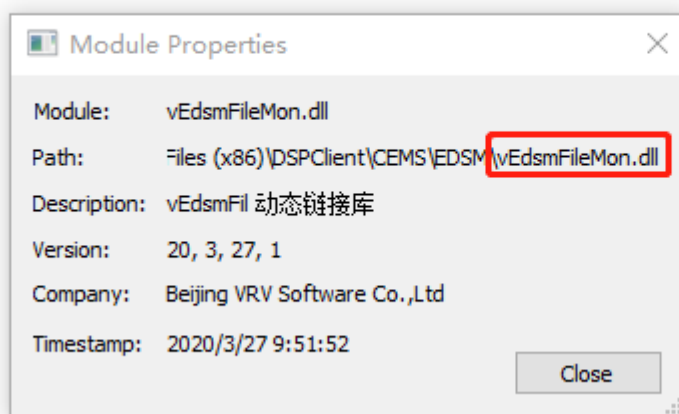
### 案例分析：

- 报错出现在 14:58:01 path:C:\Windows\SysWOW64\WerFault.exe

14:58:01.3781288	vUserHci.exe	9696	CreateFile	C:\Windows\SysWOW64\WerFault.exe
------------------	--------------	------	------------	----------------------------------

- 在堆栈信息中看到 C:\Program Files (x86)\DSPClient\CEMS\EDSM\vEdsmFileMon.dll 引入

U 38	vEdsmFileMon.dll	vEdsmFileMon.dll + 0x1c3b4	0x6dd6c3b4	C:\Program Files (x86)\DSPClient\CEMS\EDSM\vEdsmFileMon.dll
U 39	vEdsmFileMon.dll	vEdsmFileMon.dll + 0x1c415	0x6dd6c415	C:\Program Files (x86)\DSPClient\CEMS\EDSM\vEdsmFileMon.dll



- 再报错位置向上查看，发现有大量 NotfiyChangeDirectory 条目，猜测应该 vUserHci.exe 对 C:\进行监测，但具体行为需要 vUserHci.exe 厂商进行进一步说明。

14:58:01.3223228	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3225671	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3234915	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3237079	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3246017	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3248042	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3249977	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3251278	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3260234	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3262413	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3271729	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3273710	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3274685	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3276956	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3286480	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3288620	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3297610	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3299608	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3300582	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3302650	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3311799	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3313921	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3322694	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3326698	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3327879	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3332692	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3344198	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE
14:58:01.3346848	vUserHci.exe	9696	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE

# Event Properties

Event Process Stack

## Image



VPEngine.EXE

Beijing VRV Software Co.,Ltd

Name: vUserHci.exe

Version: 8, 1, 1901, 714

Path:

C:\Program Files (x86)\DSPClient\CEMS\vUserHci.exe

Command Line:

"C:\Program Files (x86)\DSPClient\CEMS\vUserHci.exe" -hci

PID: 9696 Architecture: 32-bit  
 Parent PID: 2624 Virtualized: False  
 Session ID: 1 Integrity: System  
 User: NT AUTHORITY\SYSTEM  
 Auth ID: 00000000:000003e7  
 Started: 2020/9/1 14:42:09 Ended: (Running)  
 Modules:

Module	Address	Size	Path
EdsmLoginTray.dll	0x6e1e0000	0x73000	C:\Program Files (x86)\DSPClient\CEMS\EDSM\EdsmLoginTray.dll
EdsmDocAuthDa...	0x6dc80000	0xc1000	C:\Program Files (x86)\DSPClient\CEMS\EDSM\EdsmDocAuthData.dll
vMarkSecTip.dll	0x6dda0000	0x21000	C:\Program Files (x86)\DSPClient\CEMS\EDSM\vMarkSecTip.dll
LIBEAY32.dll	0x10000000	0x13e000	C:\Program Files (x86)\DSPClient\CEMS\LIBEAY32.dll
libcurl.dll	0x71ac0000	0x180000	C:\Program Files (x86)\DSPClient\CEMS\libcurl.dll
IndustryAll.dll	0x4f40000	0x89000	C:\Program Files (x86)\DSPClient\CEMS\IndustryAll.dll
KDUI32.dll	0x5030000	0x2bc000	C:\Program Files (x86)\DSPClient\CEMS\KDUI32.dll
KernelAll.dll	0x5be0000	0x31a000	C:\Program Files (x86)\DSPClient\CEMS\KernelAll.dll
AdvancedAll.dll	0x5f00000	0x9c000	C:\Program Files (x86)\DSPClient\CEMS\AdvancedAll.dll
OfficeAll.dll	0x5fa0000	0x9f000	C:\Program Files (x86)\DSPClient\CEMS\OfficeAll.dll
DirectUI.dll	0x6040000	0xc3000	C:\Program Files (x86)\DSPClient\CEMS\DirectUI.dll

## Company

北京北信源软件  
 TODO: <公司名>  
 TODO: <Company  
 The OpenSSL Proj  
 The curl library, ht  
 Shanghai YongJin  
 Shanghai YongJin  
 Shanghai YongJin  
 Shanghai YongJin  
 Shanghai YongJin  
 Shanghai YongJin



# Event Properties

Event Process Stack

## Image



VPEngine.EXE

Beijing VRV Software Co.,Ltd

Name: vUserHci.exe

Version: 8, 1, 1901, 714

Path:

C:\Program Files (x86)\DSPClient\CEMS\vUserHci.exe

Command Line:

"C:\Program Files (x86)\DSPClient\CEMS\vUserHci.exe" -hci

PID: 9696 Architecture: 32-bit  
Parent PID: 2624 Virtualized: False  
Session ID: 1 Integrity: System  
User: NT AUTHORITY\SYSTEM  
Auth ID: 00000000:000003e7  
Started: 2020/9/1 14:42:09 Ended: (Running)  
Modules:

Module	Address	Size	Path	Company
CRYPT32.dll	0x76e20000	0x199000	C:\Windows\SysWOW64\CRYPT32.dll	Microsoft Corporat
bcrypt.dll	0x76fc0000	0x19000	C:\Windows\SysWOW64\bcrypt.dll	Microsoft Corporat
profapi.dll	0x76fe0000	0x1c000	C:\Windows\SysWOW64\profapi.dll	Microsoft Corporat
gdi32full.dll	0x77070000	0x166000	C:\Windows\SysWOW64\gdi32full.dll	Microsoft Corporat
CRYPTSP.dll	0x77200000	0x12000	C:\Windows\SysWOW64\CRYPTSP.dll	Microsoft Corporat
combase.dll	0x772b0000	0x278000	C:\Windows\SysWOW64\combase.dll	Microsoft Corporat
wow64cpu.dll	0x77530000	0x9000	C:\Windows\System32\wow64cpu.dll	Microsoft Corporat
ntdll.dll	0x77540000	0x19c000	C:\Windows\SysWOW64\ntdll.dll	Microsoft Corporat
wow64.dll	0x77fcadb0000	0x53000	C:\Windows\System32\wow64.dll	Microsoft Corporat
wow64win.dll	0x77fcae320...	0x7c000	C:\Windows\System32\wow64win.dll	Microsoft Corporat
ntdll.dll	0x77fcb0380...	0x1ed000	C:\Windows\SYSTEM32\ntdll.dll	Microsoft Corporat
EdpCrypt.dll	0x13e0000	0x1a000	C:\Program Files (x86)\DSPClient\CEMS\EDSM\EdpCrypt.dll	EDP
vUserHci.exe	0x11f0000	0x2f000	C:\Program Files (x86)\DSPClient\CEMS\vUserHci.exe	Beijing VRV Softwa
vCemsSrv.dll	0x2c10000	0x123000	C:\Program Files (x86)\DSPClient\CEMS\vCemsSrv.dll	Beijing VRV Softwa
vSelfSafe.dll	0x35b0000	0x59000	C:\Program Files (x86)\DSPClient\common\vSelfSafe.dll	Beijing VRV Softwa
ckfiles.dll	0x6dc10000	0x67000	C:\Program Files (x86)\DSPClient\CEMS\EDSM\ckfiles.dll	Beijing VRV Softwa
vEdsmFileMon.dll	0x6dd50000	0x48000	C:\Program Files (x86)\DSPClient\CEMS\EDSM\vEdsmFileMon.dll	Beijing VRV Softwa
vCemsPlc.dll	0x6e590000	0xb1000	C:\Program Files (x86)\DSPClient\CEMS\vCemsPlc.dll	Beijing VRV Softwa
EnsecCore.dll	0x6e660000	0x61000	C:\Program Files (x86)\DSPClient\CEMS\EDSM\EnsecCore.dll	Beijing VRV Softwa
VRVTrustVerify.dll	0x6e960000	0x55000	C:\Program Files (x86)\DSPClient\common\VRVTrustVerify.dll	Beijing VRV Softwa
vEdpIpc.dll	0x74a70000	0x2a000	C:\Program Files (x86)\DSPClient\CEMS\vEdpIpc.dll	Beijing VRV Softwa
vMainBus.dll	0x74aa0000	0x31000	C:\Program Files (x86)\DSPClient\CEMS\vMainBus.dll	Beijing VRV Softwa
vSysNtfy.dll	0x74b20000	0x21000	C:\Program Files (x86)\DSPClient\CEMS\vSysNtfy.dll	Beijing VRV Softwa
vDbgMgr.dll	0x74b50000	0x38000	C:\Program Files (x86)\DSPClient\CEMS\vDbgMgr.dll	Beijing VRV Softwa
cemsStore.dll	0x2fd0000	0x1d2000	C:\Program Files (x86)\DSPClient\CEMS\cemsStore.dll	
vCemsOnLine.dll	0x4c50000	0x118000	C:\Program Files (x86)\DSPClient\CEMS\vCemsOnLine.dll	
cemsBase.dll	0x4df0000	0x4d000	C:\Program Files (x86)\DSPClient\CEMS\cemsBase.dll	
vGlog.dll	0x6ddd0000	0x55000	C:\Program Files (x86)\DSPClient\CEMS\EDSM\vGlog.dll	
ClientVerifyFunc...	0x6e650000	0xf000	C:\Program Files (x86)\DSPClient\CEMS\EDSM\ClientVerifyFuncEX.dll	

Event Properties				
Event Process Stack				
Frame	Module	Location	Address	Path
K 0	FLTMGR.SYS	FLTMGR.SYS + 0x555d	0xfffff8053a40555d	C:\Windows\System32\drivers\FLTMGR.SYS
K 1	FLTMGR.SYS	FLTMGR.SYS + 0x50bc	0xfffff8053a4050bc	C:\Windows\System32\drivers\FLTMGR.SYS
K 2	FLTMGR.SYS	FLTMGR.SYS + 0x4c28	0xfffff8053a404c28	C:\Windows\System32\drivers\FLTMGR.SYS
K 3	FLTMGR.SYS	FLTMGR.SYS + 0x4a1e	0xfffff8053a404a1e	C:\Windows\System32\drivers\FLTMGR.SYS
K 4	ntoskrnl.exe	ntoskrnl.exe + 0x78b99	0xfffff80537b2cb99	C:\Windows\system32\ntoskrnl.exe
K 5	ntoskrnl.exe	ntoskrnl.exe + 0x5f6b11	0xfffff805380aab11	C:\Windows\system32\ntoskrnl.exe
K 6	ntoskrnl.exe	ntoskrnl.exe + 0x5bc349	0xfffff80538070349	C:\Windows\system32\ntoskrnl.exe
K 7	ntoskrnl.exe	ntoskrnl.exe + 0x5bc0ac	0xfffff805380700ac	C:\Windows\system32\ntoskrnl.exe
K 8	ntoskrnl.exe	ntoskrnl.exe + 0x1c5305	0xfffff80537c79305	C:\Windows\system32\ntoskrnl.exe
U 9	ntdll.dll	ntdll.dll + 0xa1974	0x7ffcb0421974	C:\Windows\SYSTEM32\ntdll.dll
U 10	wow64.dll	wow64.dll + 0x29888	0x7ffcadbe9888	C:\Windows\System32\wow64.dll
U 11	wow64.dll	wow64.dll + 0x7783	0x7ffcadbc7783	C:\Windows\System32\wow64.dll
U 12	wow64cpu.dll	wow64cpu.dll + 0x1783	0x77531783	C:\Windows\System32\wow64cpu.dll
U 13	wow64cpu.dll	wow64cpu.dll + 0x1199	0x77531199	C:\Windows\System32\wow64cpu.dll
U 14	wow64.dll	wow64.dll + 0xcfd4	0x7ffcadbccfd4	C:\Windows\System32\wow64.dll
U 15	wow64.dll	wow64.dll + 0xf182	0x7ffcadbcf182	C:\Windows\System32\wow64.dll
U 16	wow64.dll	wow64.dll + 0xf1ef	0x7ffcadbcf1ef	C:\Windows\System32\wow64.dll
U 17	ntdll.dll	ntdll.dll + 0xa33ce	0x7ffcb04233ce	C:\Windows\SYSTEM32\ntdll.dll
U 18	wow64cpu.dll	wow64cpu.dll + 0x1cbc	0x77531cbc	C:\Windows\System32\wow64cpu.dll
U 19	wow64cpu.dll	wow64cpu.dll + 0x1b99	0x77531b99	C:\Windows\System32\wow64cpu.dll
U 20	wow64cpu.dll	wow64cpu.dll + 0x1199	0x77531199	C:\Windows\System32\wow64cpu.dll
U 21	wow64.dll	wow64.dll + 0xcfd4	0x7ffcadbccfd4	C:\Windows\System32\wow64.dll
U 22	wow64.dll	wow64.dll + 0xcea0	0x7ffcadbcc0ea0	C:\Windows\System32\wow64.dll
U 23	ntdll.dll	ntdll.dll + 0x757db	0x7ffcb03f57db	C:\Windows\SYSTEM32\ntdll.dll
U 24	ntdll.dll	ntdll.dll + 0x756c3	0x7ffcb03f56c3	C:\Windows\SYSTEM32\ntdll.dll
U 25	ntdll.dll	ntdll.dll + 0x7566e	0x7ffcb03f566e	C:\Windows\SYSTEM32\ntdll.dll
U 26	ntdll.dll	ntdll.dll + 0x715bc	0x775b15bc	C:\Windows\SysWOW64\ntdll.dll
U 27	vEdsmFileMon.dll	vEdsmFileMon.dll + 0x2e7c	0x6dd52e7c	C:\Program Files (x86)\DSPClient\CEMS
U 28	vEdsmFileMon.dll	vEdsmFileMon.dll + 0x11a2	0x6dd511a2	C:\Program Files (x86)\DSPClient\CEMS
U 29	vEdsmFileMon.dll	vEdsmFileMon.dll + 0x1c1fb	0x6dd6c1fb	C:\Program Files (x86)\DSPClient\CEMS
U 30	KERNEL32.DLL	KERNEL32.DLL + 0x20419	0x75a10419	C:\Windows\SysWOW64\KERNEL32.DLL
U 31	ntdll.dll	ntdll.dll + 0x6662d	0x775a662d	C:\Windows\SysWOW64\ntdll.dll
U 32	ntdll.dll	ntdll.dll + 0x665fd	0x775a65fd	C:\Windows\SysWOW64\ntdll.dll

- 从补丁安装角度分析，安装 Windows Update 过程中，文件相关行为主要集中在 C:\Windows\servicing\InboxFodMetadataCache、C:\Windows\servicing\InboxFodMetadataCache\metadata、和 C:\Windows\SoftwareDistribution\Download 文件夹下。有大量文件写入、读取请求信息等操作。

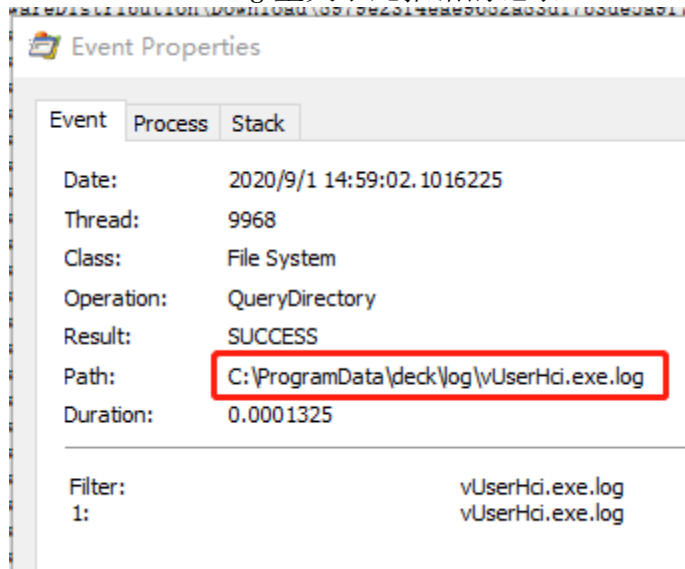
14:57:02.0130640	TiWorker.exe	7192	CreateFile	C:\Windows\servicing\InboxFodMet
14:57:02.0130867	TiWorker.exe	7192	QueryBasicInformationFile	C:\Windows\servicing\InboxFodMet
14:57:02.0131153	TiWorker.exe	7192	CloseFile	C:\Windows\servicing\InboxFodMet
14:57:02.0227387	TiWorker.exe	7192	CreateFile	C:\Windows\servicing\InboxFodMet
14:57:02.0227936	TiWorker.exe	7192	QueryStandardInformationFile	C:\Windows\servicing\InboxFodMet
14:57:02.0343704	TiWorker.exe	7192	CreateFile	C:\Windows\servicing\InboxFodMet
14:57:02.0343956	TiWorker.exe	7192	QuerySecurityFile	C:\Windows\servicing\InboxFodMet
14:57:02.0344178	TiWorker.exe	7192	QueryStandardInformationFile	C:\Windows\servicing\InboxFodMet
14:57:02.0344553	TiWorker.exe	7192	ReadFile	C:\Windows\servicing\InboxFodMet
14:57:02.0344833	TiWorker.exe	7192	CloseFile	C:\Windows\servicing\InboxFodMet
14:57:02.0427096	TiWorker.exe	7192	CreateFile	C:\Windows\servicing\InboxFodMet
14:57:02.0427640	TiWorker.exe	7192	QueryStandardInformationFile	C:\Windows\servicing\InboxFodMet
14:57:02.0428242	TiWorker.exe	7192	ReadFile	C:\Windows\servicing\InboxFodMet
14:57:02.0428898	TiWorker.exe	7192	CloseFile	C:\Windows\servicing\InboxFodMet
14:57:14.5324890	TiWorker.exe	7192	ReadFile	C:\Windows\SoftwareDistribution\
14:57:14.5324996	TiWorker.exe	7192	ReadFile	C:\Windows\SoftwareDistribution\
14:57:14.5325108	TiWorker.exe	7192	ReadFile	C:\Windows\SoftwareDistribution\
14:57:14.5325201	TiWorker.exe	7192	ReadFile	C:\Windows\SoftwareDistribution\
14:57:14.5327959	TiWorker.exe	7192	CreateFile	C:\Windows\SoftwareDistribution\
14:57:14.5328117	TiWorker.exe	7192	QueryBasicInformationFile	C:\Windows\SoftwareDistribution\
14:57:14.5328315	TiWorker.exe	7192	CloseFile	C:\Windows\SoftwareDistribution\
14:57:14.5331634	TiWorker.exe	7192	CreateFile	C:\Windows\SoftwareDistribution\
14:57:14.5331358	TiWorker.exe	7192	QueryBasicInformationFile	C:\Windows\SoftwareDistribution\

### 建议操作：

- 1) vUserHci.exe 厂商进行进一步说明 vUserHci.exe 的功能和大量 NotfiyChangeDirectory 条目的具体行为。
- 2) 如果针对 C:\全盘进行文件检测或保护等行为，是否可以先将 C:\Windows\servicing\InboxFodMetadataCache、C:\Windows\servicing\InboxFodMetadataCache\metadata、和 C:\Windows\SoftwareDistribution\Download 文件夹加入例外，尝试问题是否复现。如果问题不再复现，可以逐一扩大定位位置。



3) Log 中发现 vUserHci.exe 会写 Log, 所以请 vUserHci.exe 厂商查看 vUserHci.exe.log 里关于此报错的记录。



#### 数据收集:

此外, 补丁安装过程会在 CBS.log 记录。我可以尝试从入下日志寻找安装失败问题的信息。

- 复现问题现象, 并记录时间点, 随后收集上传如下日志。

C:\Windows\Logs\CBS\CBS.log

C:\Windows\Logs\CBS\dism.log

C:\Windows\System32\winevt\Logs\Application.evtx

C:\Windows\System32\winevt\Logs\System.evtx

-----  
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](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

发件人: [win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn) <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

发送时间: 2020 年 9 月 1 日 17:50

收件人: [win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)

抄送: Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>; CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>; Liu Wei

<[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>; Qi Feng <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>; Wang Dan <[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>;  
Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>

主题: 答复: 回复: 回复: [案例号: CAS-02878-F9R9D5 ] % |P2|ICBC|在 8 月补丁安装失败过程中弹出  
vuser.exe % 初次响应 CMIT:0001892

下午 2.58 分左右。

发件人: win10 升级支持/系统一部/软件开发中心/ICBC  
收件人: Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>  
抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>, Liu Wei <[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>, Qi Feng <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>, Wang Dan  
<[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>, Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>  
日期: 2020/09/01 16:50  
主题: 答复: 回复: 回复: [案例号: CAS-02878-F9R9D5 ] % |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应  
CMIT:0001892

---

时间大概在 3 点 10-20 分左右

发件人: Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>  
收件人: "[win10sup@sdc.icbc.com.cn](mailto:win10sup@sdc.icbc.com.cn)" <[win10sup@sdc.icbc.com.cn](mailto:win10sup@sdc.icbc.com.cn)>  
抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>, Liu Wei <[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>, Qi Feng <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>, Wang Dan  
<[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>, Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>  
日期: 2020/09/01 16:47  
主题: 回复: 回复: [案例号: CAS-02878-F9R9D5 ] % |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应  
CMIT:0001892

---

吴先生，您好！

收到，我正在下载。此外出现弹框报错的具体时间点您可以通过邮件反馈，谢谢。

-----  
-----

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](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

发件人: [win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn) <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

发送时间: 2020 年 9 月 1 日 16:21

收件人: Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>

抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>; Liu Wei <[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>; Qi Feng <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>; Wang Dan <[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>; Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>

主题: 答复: 回复: [案例号: CAS-02878-F9R9D5 ] % |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应 CMIT:0001892

贾工, 日志通过 FTP 上传至 DUMP/补丁安装失败  
请注意查收

发件人: Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>

收件人: 吴毓杰 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>, Liu Wei <[liuwei@cmgos.com](mailto:liuwei@cmgos.com)>, Qi Feng <[qifeng@cmgos.com](mailto:qifeng@cmgos.com)>, Wang Dan <[wangdan@cmgos.com](mailto:wangdan@cmgos.com)>, Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>

日期: 2020/08/31 18:03

主题: 回复: [案例号: CAS-02878-F9R9D5 ] % |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应 CMIT:0001892

---

吴先生, 您好!

由于本地环境未能复现 vuser.exe 弹框报错的问题现象, 还需要您提供如下数据以供进一步定位分析。

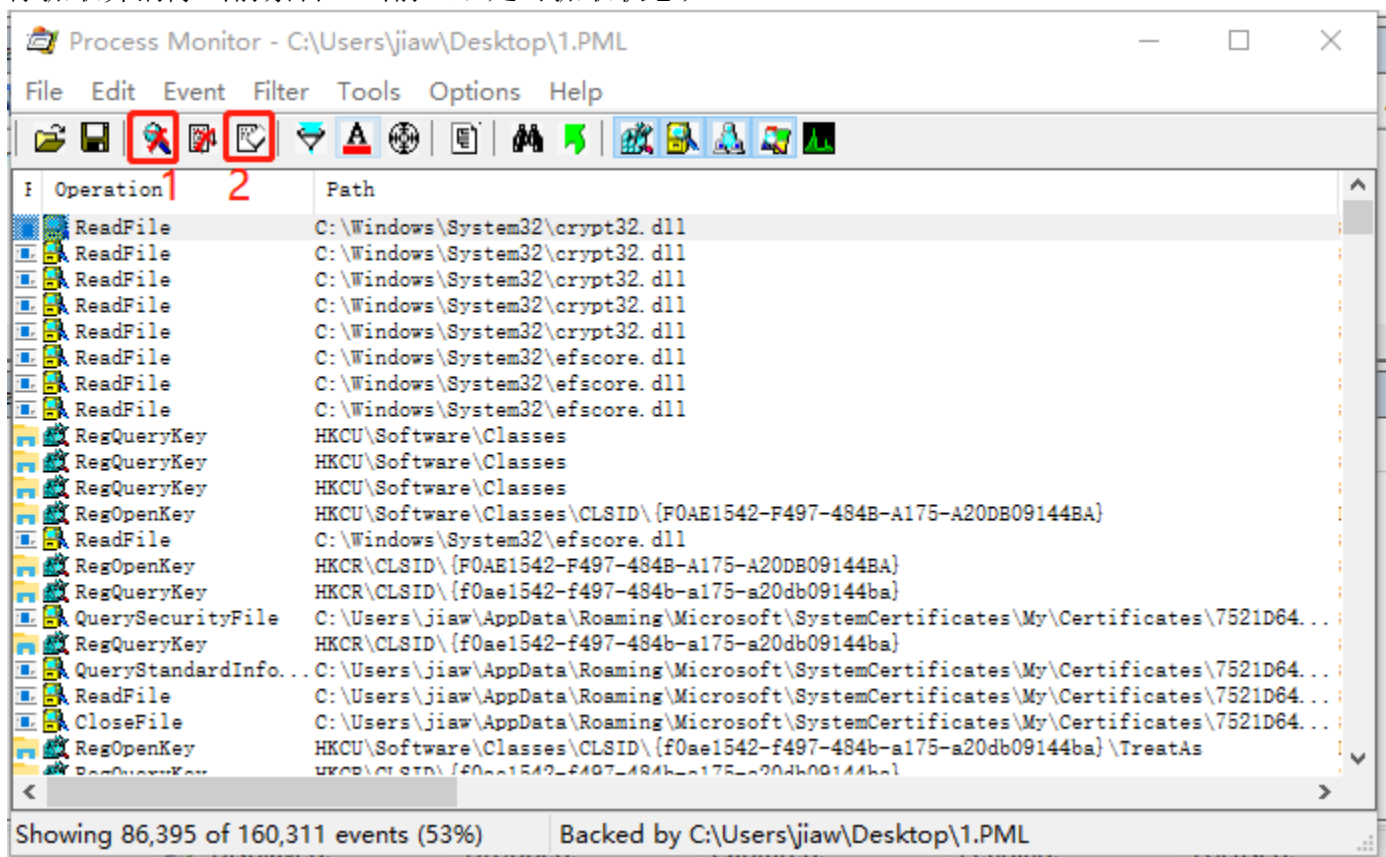
### 数据收集:

- 一、提示报错的截图或照片;
- 二、抓取 Procmon 日志;

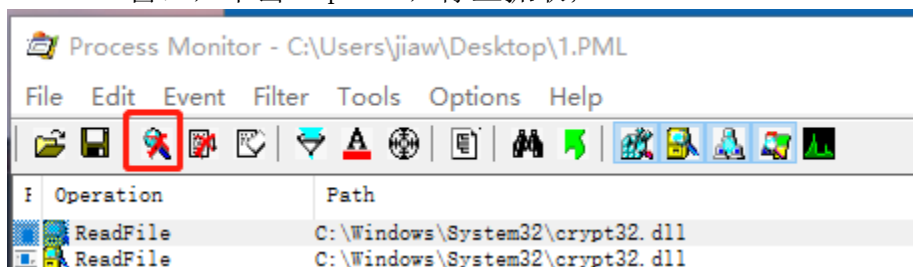
在出现安装升级 patch 报错的 V0-H 1020 版本机器上进行如下操作:

- 1) 请下载并解压附件;
- 2) 双击 Procmon.exe 运行, 到达此页面, 会有大量条目出现, 先后点击 1, 2 暂

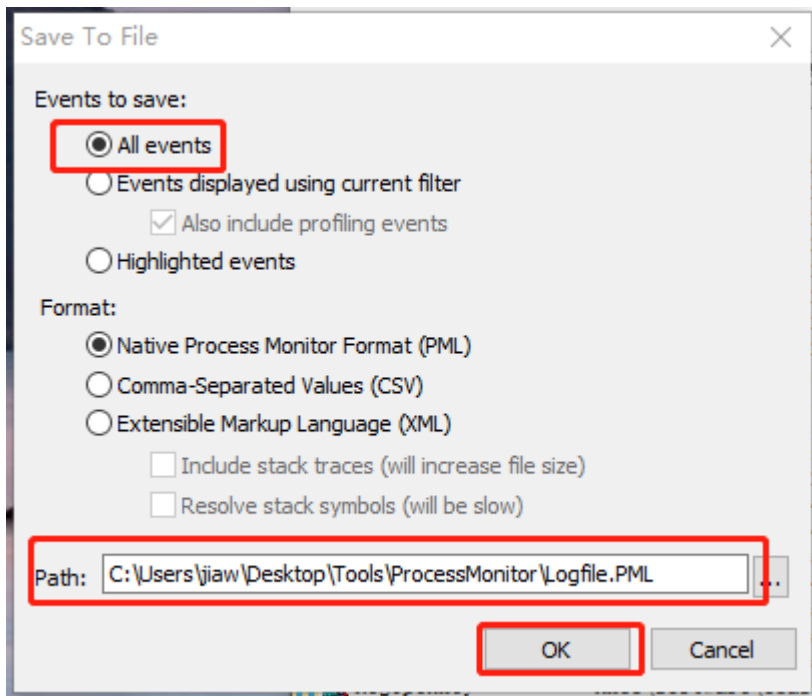
停抓取并清除当前条目。当前已经是可抓取状态；



3) 准备好复现条件，点击下图的图标开始抓取。复现问题，记录时间点（对于案例分析极为重要。例如出现弹框报错的时间点），出现问题现象后。回到 Process Monitor 窗口，单击 Capture，停止抓取；



4) 点击 File，点击 Save。选择“All events” and “Native Process Monitor Format (PML)”点击 OK。记录文件保存位置；



5) 分别将上述照片和 PML 文件打包压缩。

#### 数据上传:

为了更安全、快速地传输数据，您可以在 Filezilla 上使用以下账户信息登入神州网信网站。

l Filezilla client 端下载 URL: <https://filezilla-project.org/download.php?type=client>

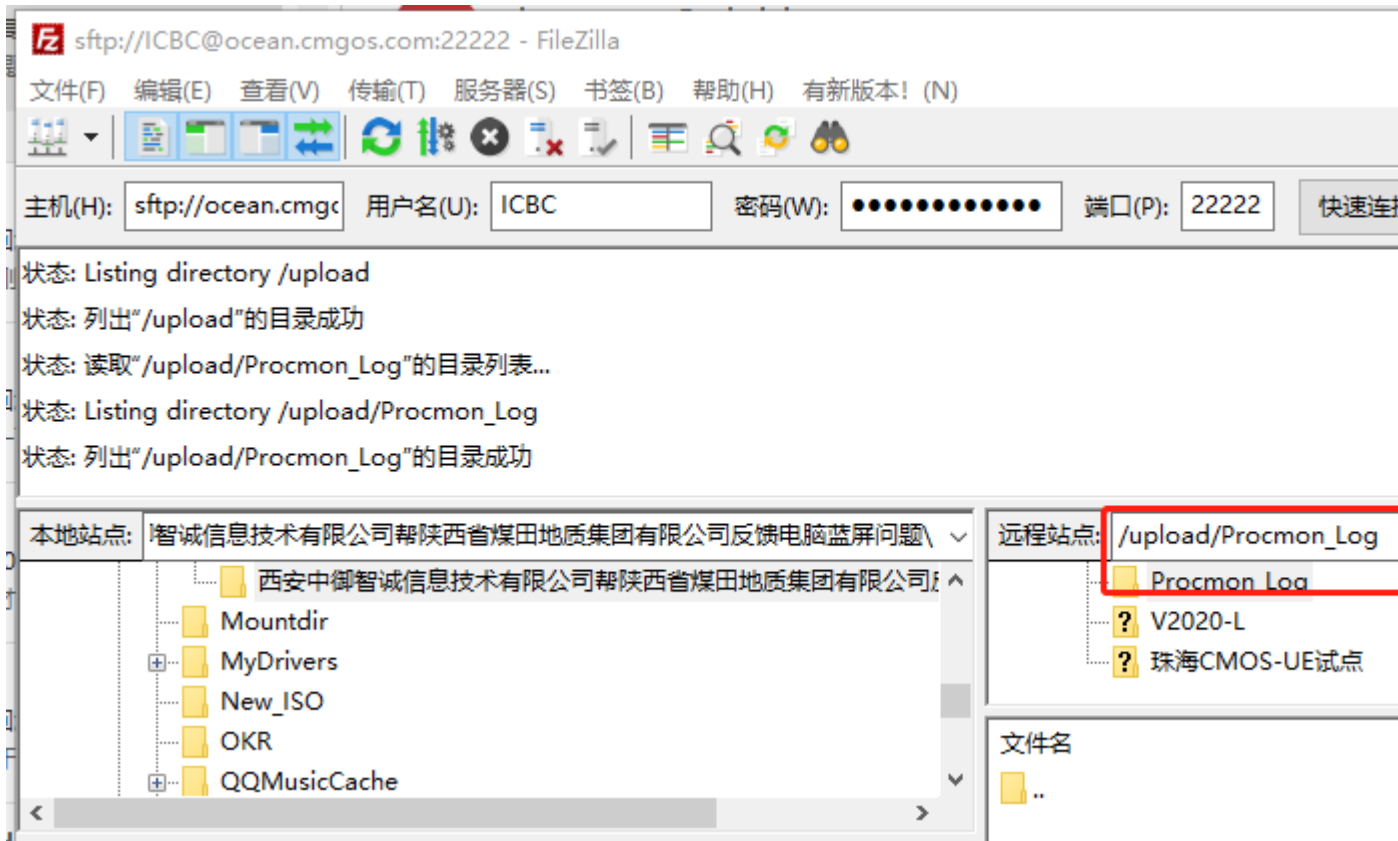
l 登陆地址: sftp://ocean.cmgos.com

l 用户名为: ICBC (区分大小写)

l 密码: 2qfs52ninbFB

l 端口: 22222

登陆之后，上传至/upload/Procmon\_Log 文件夹



-----  
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](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

发件人: Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>

发送时间: 2020 年 8 月 31 日 15:46

收件人: 吴毓杰 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

抄送: Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>

主题: [案例号: CAS-02878-F9R9D5 ] % |P2|ICBC|在 8 月补丁安装失败过程中弹出 vuser.exe % 初次响应 CMIT:0001892

吴毓杰 先生/女士, 您好!

感谢您联系神州网信技术支持中心。我是技术支持工程师 贾伟 。很高兴能有机会协助您解决该问题。 您可随时通过邮件回复以及该问题事件号码 CAS-02878-F9R9D5 与我联系。

如果您有任何其他疑问，请随时与我联系。

此致，

敬礼

---

以上内容是一封有关向神州网信技术有限公司提交技术支持事件的邮件。

如果您希望本次回复能够被自动加入技术支持事件中, 您可以选择“全部回复”。

[附件 “ProcessMonitor.zip” 被 win10 升级支持/系统一部/软件开发中心/ICBC 删除]

---

此邮件信息仅供收件人查阅，所含任何评论、陈述或数据仅供收件人参考，若有改动，恕可能不另行通知。未经中国工商银行书面许可，请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件，敬请及时通知发件人，并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。

This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely. The sender and ICBC are not responsible for the loss caused possibly by e-mail.

---

此邮件信息仅供收件人查阅，所含任何评论、陈述或数据仅供收件人参考，若有改动，恕可能不另行通知。未经中国工商银行书面许可，请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件，敬请及时通知发件人，并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。

This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely. The sender and ICBC are not responsible for the loss caused possibly by e-mail.

附件“KB-File\_Info.zip”被 win10 升级支持/系统一部/软件开发中心/ICBC 删除]

---

此邮件信息仅供收件人查阅，所含任何评论、陈述或数据仅供收件人参考，若有改动，恕可能不另行通知。未经中国工商银行书面许可，请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件，敬请及时通知发件人，并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。

This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely. The sender and ICBC are not responsible for the loss caused possibly by e-mail.



---

—

此邮件信息仅供收件人查阅，所含任何评论、陈述或数据仅供收件人参考，若有改动，恕可能不另行通知。未经中国工商银行书面许可，请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件，敬请及时通知发件人，并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。

This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely. The sender and ICBC are not responsible for the loss caused possibly by e-mail.