王先生，您好：

如刚才电话沟通，经您的确认，此问题将关闭，以下为案例总结，请您知悉：

Case No：CAS-06770-S3X0B3

问题描述：

==========

用户反馈 V2022-L 在使用过程中多次突然出现蓝屏重启现象。

问题分析：

==========

经日志分析，当前蓝屏问题为内存缓冲区溢出导致，与 c:\windows\system32\drivers\PCASp50.sys 文件有关，该文件版本过低，经查询，该文件存在相关安全漏洞，建议更新或卸载。

问题总结：

==========

经用户确认，卸载相关软件后，该问题得以解决，此 case 做关闭处理。

以上为此问题的案例总结，如有任何问题，可随时与我们联系，谢谢

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: Li Qi
发送时间: 2022 年 8 月 2 日 17:04
收件人: '王新国' <wangxg@shengfusm.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: 回复： 回复： [案例号: CAS-06770-S3X0B3] % 上海盛富信息技术有限公司反馈中国宝武钢铁集团有限公司用户蓝屏问题 % 初次响应 CMIT:0001295

王先生，您好：

如刚才电话沟通，请参见以下链接对于此漏洞的说明：

https://www.kb.cert.org/vuls/id/600671/#:~:text=The%20Rawether%20framework%20for%20Windows%2C%20originally%20produced%20by,vendors%20in%20their%20WiFi%20and%20router%20control%20applications.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3196

概述

PCAUSA 的 Rawether 框架没有正确验证 BPF 数据，允许精心制作的恶意 BPF 程序在驱动程序接收网络数据包的典型范围之外对内存执行操作。此漏洞可能被利用在 Windows 系统上执行本地权限提升。

描述

适用于 Windows 的 Rawether 框架最初由 Printing Communications Assoc., Inc. (PCAUSA) 生产，是一个促进应用程序与网络驱动程序接口系统(NDIS) 协议之间通信的框架。许多不同的硬件供应商在其 WiFi 和路由器控制应用程序中使用此框架。Rawether 实现了Berkeley Packet Filter (BPF) 机制。BPF 过滤器被编译成由 BPF 虚拟机执行的小程序。

CWE-119：内存缓冲区边界内的操作限制不当- CVE-2017-3196

Rawether 框架在执行前未正确验证 BPF 程序，从而允许 BPF 程序读取/写入任意内存或无限循环。堆栈上的返回地址可能会被覆盖，从而允许本地用户以 SYSTEM 权限执行任意代码。

要启用驱动程序的易受攻击部分，漏洞利用必须发出*带有NDIS_PACKET_TYPE_ALL_LOCAL标志的 OID_GEN_CURRENT_PACKET_FILTER* NDIS 请求并设置 BPF 程序。通过读取第一个接收到的网络数据包触发漏洞利用。研究人员提供了概念证明

影响 64 位版本的*PcaSp60.sys*驱动程序，该驱动程序是 ASUS PCE-AC56 WLAN 卡实用程序的一部分。但是，使用此驱动程序的其他实用程序和程序也可能会受到影响。由于驱动程序名称、版本或设备名称或信息的不同，识别易受攻击的软件可能很困难，但易受攻击的驱动程序很可能包含在 OEM WiFi 实用程序中。受影响驱动程序的一些常见默认命名约定包括：

- PcaSp60.sys
- PcaSp50.sys
- PcaMp60.sys
- PcaMp50.sys

李琦 Li Qi

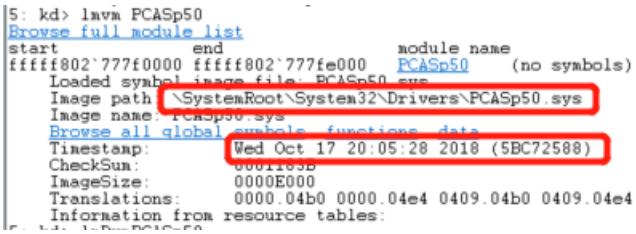
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: 王新国 <wangxg@shengfusm.com>
发送时间: 2022 年 8 月 2 日 16:27
收件人: Li Qi <liqi@cmgos.com>
主题: 回复：回复：[案例号: CAS-06770-S3X0B3] % 上海盛富信息技术有限公司反馈中国宝武钢铁集团有限公司用户蓝屏问题 % 初次响应 CMIT:0001295

发件人：Li Qi <liqi@cmgos.com>
发送时间：2022 年 8 月 2 日(星期二) 15:19
收件人：undefined <undefined>
抄　送：undefined <undefined>
主　题：回复: 回复：[案例号: CAS-06770-S3X0B3] % 上海盛富信息技术有限公司反馈中国宝武钢铁集团有限公司用户蓝屏问题 % 初次响应 CMIT:0001295

王先生，您好:

如刚才电话沟通，当前上传日志定位蓝屏问题与 c:\windows\system32\drivers\PCASp50.sys 文件有关，该文件版本过低，显示为 2018 年版本，需要进行更新。

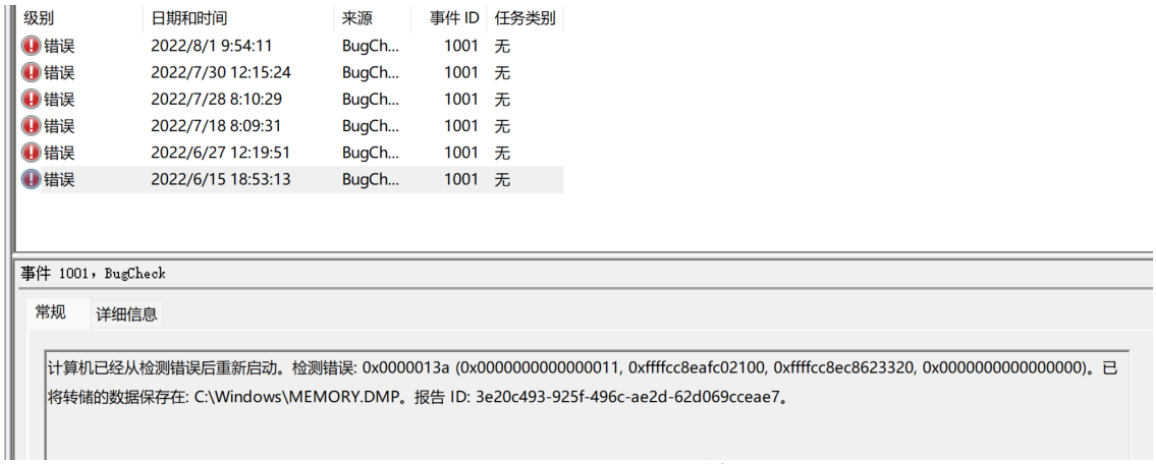


以下为 dump 分析，请您知悉:

从 bugcheck 来看，该问题为 bugcheck 0x13，且第一个参数为 11，意为内核模式堆管理器检测到堆损坏，堆在当前操作期间检测到无效的内部状态。这通常是缓冲区溢出的结果。

```
KERNEL_MODE_HEAP_CORRUPTION (13a)
The kernel mode heap manager has detected corruption in a heap.
Arguments:
Arg1: 0000000000000011, Type of corruption detected
Arg2: ffff84881b402100, Address of the heap that reported the corruption
Arg3: ffff848836235aa0, Address at which the corruption was detected
Arg4: 0000000000000000
```

且用户在之前有过多次蓝屏的记录，报错均一致。可判断为大概率由同一问题引发。



级别	日期和时间	来源	事件 ID	任务类别
错误	2022/8/1 9:54:11	BugCh...	1001	无
错误	2022/7/30 12:15:24	BugCh...	1001	无
错误	2022/7/28 8:10:29	BugCh...	1001	无
错误	2022/7/18 8:09:31	BugCh...	1001	无
错误	2022/6/27 12:19:51	BugCh...	1001	无
错误	2022/6/15 18:53:13	BugCh...	1001	无

事件 1001，BugCheck

常规　详细信息

计算机已经从检测错误后重新启动。检测错误: 0x0000013a (0x0000000000000011, 0xffffcc8eafc02100, 0xffffcc8ec8623320, 0x0000000000000000)。已将转储的数据保存在: C:\Windows\MEMORY.DMP。报告 ID: 3e20c493-925f-496c-ae2d-62d069cceae7。

查看 call stack 信息，系统调用 driver PCASp50.sys 后，释放内存时出现问题。

```
fffffaa01`b8453588 fffff802`6b98e998 : 00000000`0000013a 00000000`00000011 ffff8488`1b402100 ffff8488`36235aa0 : nt!KeBugCheckEx
fffffaa01`b8453590 fffff802`6b98e9f8 : 00000000`00000011 00000000`00000000 ffff8488`1b402100 fffffaa01`b8453638 : nt!RtlpHeapHandleErr
fffffaa01`b84535d0 fffff802`6b98e625 : 00000000`00000070 ffff8488`36235000 00000000`0000000e fffffaa01`b8453600 : nt!RtlpHpHeapHandleE
fffffaa01`b8453600 fffff802`6b825da8 : fffff802`6d4ca368 ffff8488`1eb541a0 ffff8488`0000000e ffff8488`1eb541a0 : nt!RtlpLogHeapFailur
fffffaa01`b8453630 fffff802`6b647cd2 : ffff8488`1b402340 00000000`000000ff 00000000`02000000 fffff802`00000000 : nt!RtlpHpLfhSubsegme
fffffaa01`b84536e0 fffff802`6bdb2019 : ffff8488`00000000 ffff8488`2f153030 00610038`0062002d 01000000`00100000 : nt!ExFreeHeapPool+0x
fffffaa01`b84537c0 fffff802`6d41737b : 0062002d`00350033 002d0062`00630035 ffff8488`2f153030 fffff802`777f4878 : nt!ExFreePool+0x9
fffffaa01`b84537f0 fffff802`777f13c3 : 00000000`00000000 ffff8488`36235ab0 00000000`00000000 ffff8488`2eccf080 : ndis!NdisFreeMemory+
fffffaa01`b8453820 fffff802`777f49c5 : ffff8488`29f71830 00000000`00000000 00000000`00000000 00000000`00000004 : PCASp50+0x13c3
fffffaa01`b8453850 fffff802`6b64e565 : ffff8488`1ba982a0 fffff802`6b69c4fd 00000000`00000fff fffffaa01`b8453a39 : PCASp50+0x49c5
fffffaa01`b8453880 fffff802`6ba242fa : 00000000`00000000 ffff8488`2df04370 00000000`00000000 00000000`00040008 : nt!IofCallDriver+0x5
fffffaa01`b84538c0 fffff802`6ba1477f : ffff8488`2eccf080 00000000`00000001 ffffbe0c`00000000 ffff8488`2df04340 : nt!IopCloseFile+0x17
fffffaa01`b8453950 fffff802`6ba1875c : 00000000`00000758 00000000`77c24660 00000000`03a7f558 00000000`00000000 : nt!ObCloseHandleTabl
fffffaa01`b8453a90 fffff802`6b8096b8 : ffff8488`2edf4000 ffff8488`3985ac60 fffffaa01`b8453b80 fffffaa01`b8453b80 : nt!NtClose+0xec
fffffaa01`b8453b00 00000000`77c21cfc : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!KiSystemServiceCo
00000000`0397eba8 00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : 0x77c21cfc
```


李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: Li Qi
发送时间: 2022 年 8 月 2 日 10:04
收件人: '王新国' <wangxg@shengfusm.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>

主题: 回复：[案例号：CAS-06770-S3X0B3]% 上海盛富信息技术有限公司反馈中国宝武钢铁集团有限公司用户蓝屏问题 % 初次响应 CMIT:0001295

王先生，您好：

如刚才电话沟通，我谨以此封邮件阐述我们双方针对这个问题所涉及范围界定：

问题定义:

用户反馈 V2022-L 在使用过程中多次突然出现蓝屏重启现象。

问题范围:

我们将协助您分析处理上述问题，并对定义的问题给予最大的技术支持。

如果能及时解决问题，或问题属于产品设计的行为，或问题涉及到三方，我们将考虑关闭案例。如果存在多个问题，则我们考虑拆分案例进行分析。

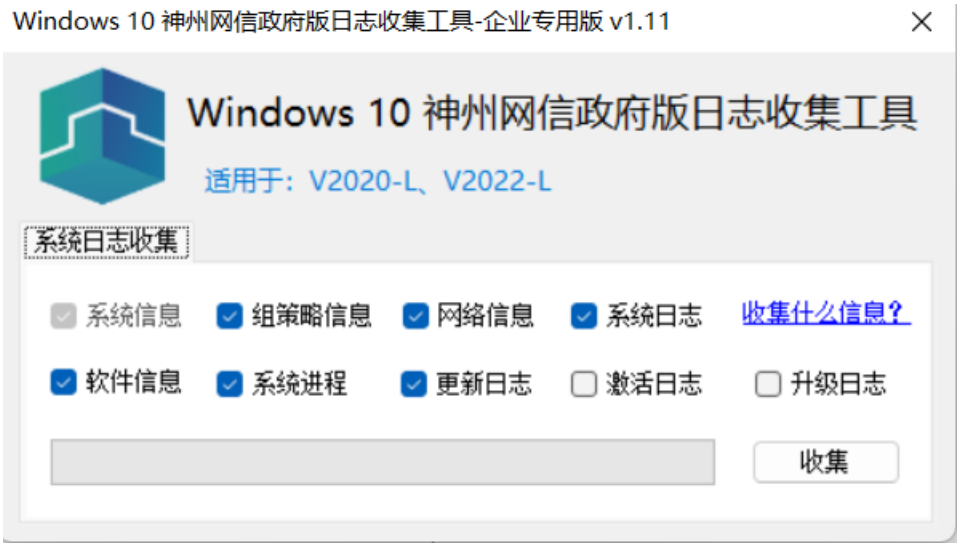
接下来，我们将开始合作解决这个问题。如果您对以上的问题范围界定有任何异议，请尽快告知。如果您有其他任何疑问。也欢迎随时与我联系。

下一步动作：

请您收取用户现场当前出现蓝屏问题的两台电脑的如下日志：

系统日志：

下载附件中的 CMGELogCollector.zip，解压后运行 CMGELogCollector.exe，点击“收集”，运行几分钟后会在桌面**生成日志压缩包**，将此日志提供给我们。



Dump 日志：

请查找 C:\windows\memory.dmp 文件是否存在，并上传至 CDUC 系统

日志上传方法：

您可以登陆 https://cduc.cmgos.com，通过数据上传系统上传您所收集的日志信息。

用户名：sfxx001

密码：sfxx001

注意：添加文件，点击上传后，跳转到新的页面点击保存。

==========

在向 CMIT 提供日志和数据前，请阅读并接受邮件下方隐私声明。

隐私声明

为向您提供本产品的相关技术支持及相关服务，您需要在同意本声明的前提下向神州网信提供为解决系统故障必要的数据和信息，包括但不限于与您相关的个人数据和隐私信息。通常情况下，我们仅需要如下数据以使我们的服务能够更好地满足您的需求：内存转储文件、注册表信息、组策略信息、事件日志、安装应用列表、驱动信息、网络日志或系统补丁等。

神州网信承诺将采取商业上可行及必要措施保护用户提供给神州网信的数据和信息，且仅在解决问题过程中使用。

神州网信保证不对外公开或向第三方提供、公开或共享您提供的数据和信息。

在以下情况下，神州网信对您的数据和信息的披露将不视为违约，具体包括：

(1) 神州网信已获得您的明确授权；

(2) 根据适用法律的要求，神州网信负有披露义务的；

(3) 司法机关或行政机关基于法定程序要求神州网信提供的；

(4) 为维护社会公共利益及神州网信合法权益，在合理范围内进行披露的。

(5) 为了解决您的系统故障问题，神州网信可能会与神州网信的分包商披露您提供的数据和信息。在此情况下，第三方会承担与神州网信同等的隐私保护责任的，神州网信会在合理范围内对您的信息进行披露。

如果您欲提供的数据和信息中包含对您重要的保密信息以及商业秘密，在您向神州网信提供上述数据和信息前，务必对上述数据和信息进行脱敏处理，否则请不要提供该信息给神州网信。作为一家商业软件公司，神州网信在商业可行的前提下，已为用户的数据和信息保护做了极大

的努力，但是仍然不能保证现有的安全技术措施使您的数据和信息等不受任何形式的损失。您对上述情况充分知情，且不会因此追究神州网信的法律责任。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: 王新国 <wangxg@shengfusm.com>
发送时间: 2022 年 8 月 1 日 17:56
收件人: Li Qi <liqi@cmgos.com>
主题: 回复：[案例号：CAS-06770-S3X0B3]％ 上海盛富信息技术有限公司反馈中国宝武钢铁集团有限公司用户蓝屏问题 ％初次响应 CMIT:0001295

上午发的邮箱问题又解决办法吗

发件人：Li Qi <liqi@cmgos.com>
发送时间：2022 年 8 月 1 日(星期一) 17:51
收件人：undefined <undefined>
主　题：[案例号: CAS-06770-S3X0B3] % 上海盛富信息技术有限公司反馈中国宝武钢铁集团有限公司用户蓝屏问题 % 初次响应 CMIT:0001295

王新国 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 李琦 。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-06770-S3X0B3 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”。