

## NVIDIA GeForce Experience漏洞分析：从任意文件写入到命令执行

### 0x00 概要

本文详细介绍了NVIDIA GeForce Experience (GFE)中多个任意文件写入漏洞（CVE-2019-5674）的发现过程，这款软件会默认安装到运行NVIDIA GeForce产品的系统上。具备任意文件写入权限后，攻击者可以强制应用程序以高权限用户身份覆盖系统上的任意文件。通常情况下，这种漏洞只能让攻击者覆盖系统关键文件，GFE会以SYSTEM用户身份将数据写入日志文件中，由于日志文件所设置的权限并不安全，因此该漏洞可以允许攻击者覆盖任意系统文件。此外，用户可以控制某个日志文件。

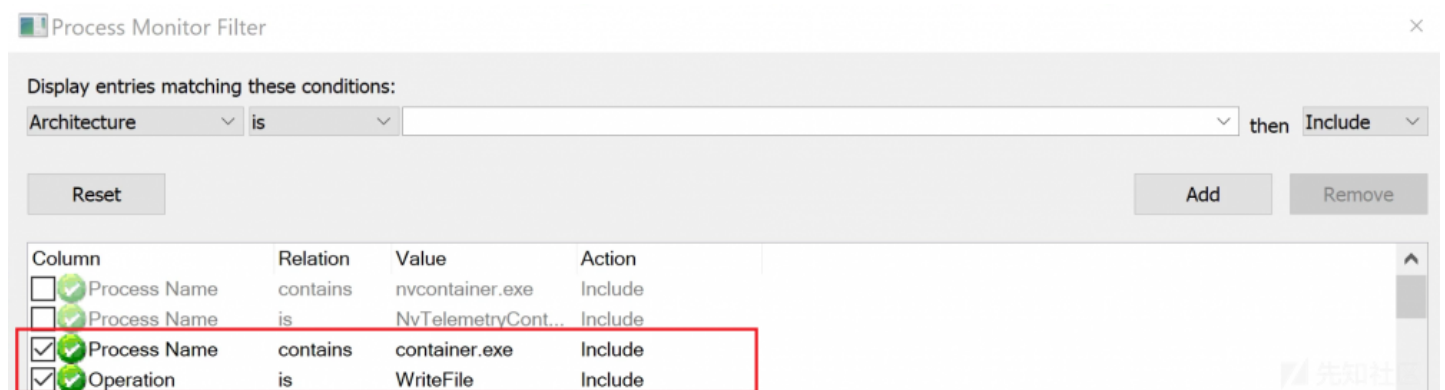
### 0x01 NVIDIA GeForce Experience GFE

根据NVIDIA官网的介绍，GeForce Experience GFE可以用来“录制视频、截图并与朋友们共享，保持驱动程序处于最新版本，并且能够优化游戏设置”。本质上这是与GeForce一起安装的一款补充应用程序，可以给用户提供

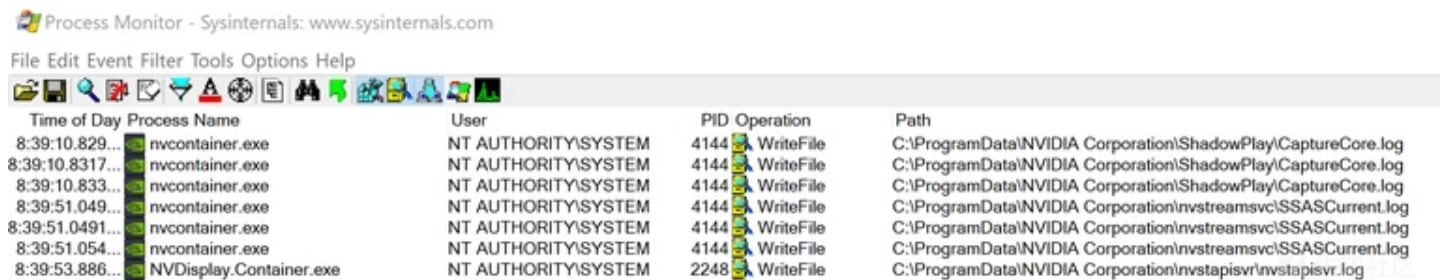
### 0x02 漏洞发现过程

为了探索当前系统中NVIDIA服务及应用中是否存在问题，我打开Process Monitor (Procmon, 来自Sysinternals的一款工具) 工具，了解默认情况下GeForce Experience及其他服务正在运行的一些应用。经过分析后，我注意到了与NVIDIA有关的几个进程：nvcontainer.exe以及NVIDIA.Container.exe。

发现NVIDIA正在运行的这些进程后，我在Procmon中添加了一个过滤器，查找\*container.exe正在写入的一些文件（使用通配符能匹配这两个程序）。



应用过滤器后，我只关注WriteFile操作，结果找到了几个可疑的目标。如下图所示，这些程序会以NT AUTHORITY\SYSTEM权限将一些日志文件写入C:\ProgramData目录中（该目录经常包含普通用户能够修改的一些文件）。



检查这些文件的权限设置后，我们发现Everyone用户组具备这些文件的完全访问权限。

因此，程序会以SYSTEM权限写入这些文件，并且Everyone能够完全控制这些文件。这里的问题在于，每个人都可以以任意方式修改文件，包括创建指向系统上其他文件的links）。如果我们能创建指向其他系统文件的链接（以正常用户身份无法写入这些文件），那么SYSTEM进程就会跟随该链接，认为这本来是应当正常写入数据的日志文件，

### 0x03 利用文件写入漏洞

我们可以利用James

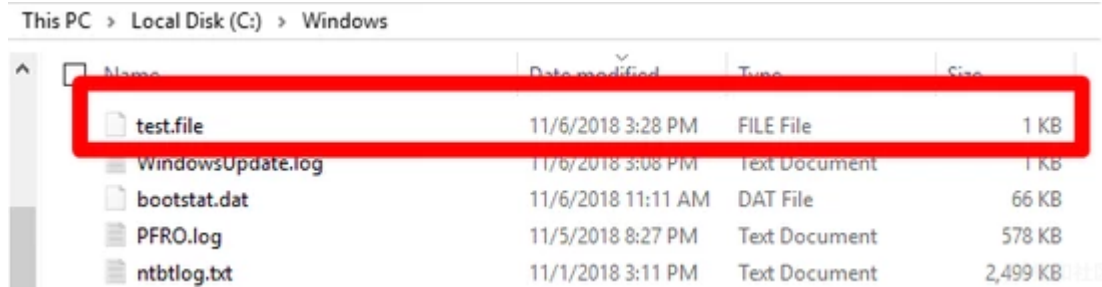
Forshaw开发的symboliclink-testing-tools来创建符号链接及硬链接，以便利用这个文件写入漏洞。这些工具可以让我们以普通用户身份创建指向系统文件的链接。在测试Corporation\nvstapivr\nvstapivr.log指向C:\windows\test.file的一个临时符号链接（只有管理员才能写入test.file）。为了成功创建符号链接，C:\Corporation\nvstapivr必须是一个空目录（这是因为该工具使用了junction技术，而这要求目录为空目录）。我们依次测试了目录不为空和为空时的效果，如下图所示

```
C:\ProgramData\NVIDIA Corporation>createsymlink nvstapisvr\nvstapisvr.log c:\windows\test.file
Error creating junction 145

C:\ProgramData\NVIDIA Corporation>createsymlink nvstapisvr\nvstapisvr.log c:\windows\test.file
Opened Link \RPC Control\nvstapisvr.log -> \??\c:\windows\test.file: 00000154
Press ENTER to exit and delete the symlink
```

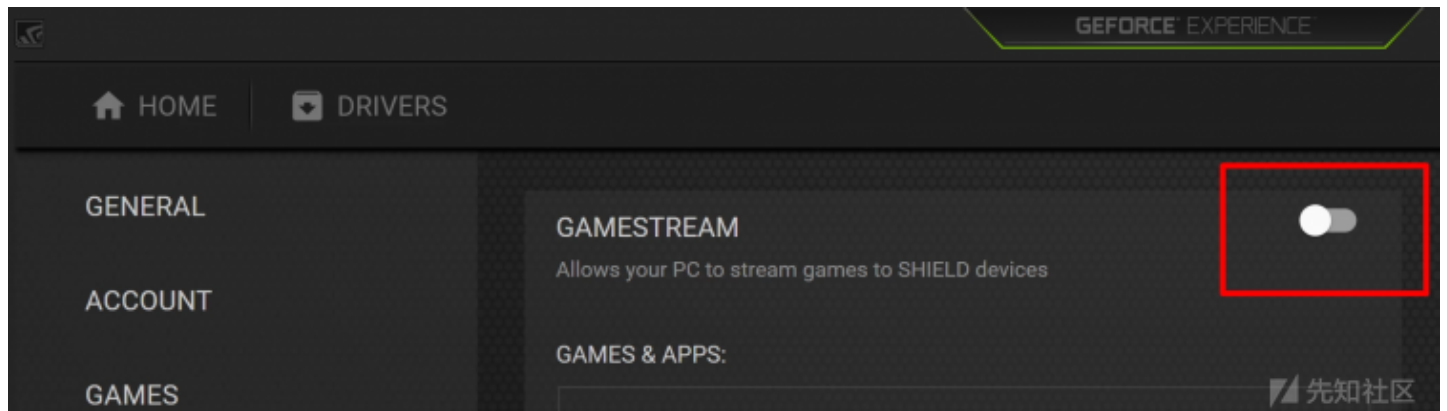
先知社区

现在，当高权限的NVIDIA进程写入C:\ProgramData\NVIDIA Corporation\nvstapisvr\nvstapisvr.log这个日志文件时，实际上写入的目的文件为C:\windows\test.file。



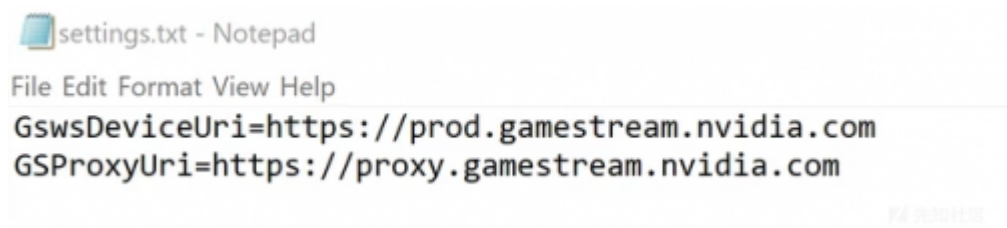
上图表明，我们可以覆盖系统上的任意文件。这的确是一个问题，但并不那么令人兴奋，因为我们无法完成更多任务，只能简单地破坏某些文件，最终可能实现DoS效果。

因此我想看看是否能够控制写入这些日志文件中的数据内容，顺便执行其他操作（如将命令写入.bat文件中）。经过一番研究后，我发现C:\ProgramData\NVIDIA Corporation\nvstreamsvc\nvstreamsvcCurrent.log中包含我在其他文件中见过的某些字符串，而我能够以普通用户身份写入这些文件。该文件为C:\ProgramData\NVIDIA Corporation\NvStreamSrv\settings.txt，其中包含一些变量，当我们打开和关闭GeForce Experience中的“GameStream”服务时，就会将这些变量写入nvstreamsvcCurrent日志文件中。

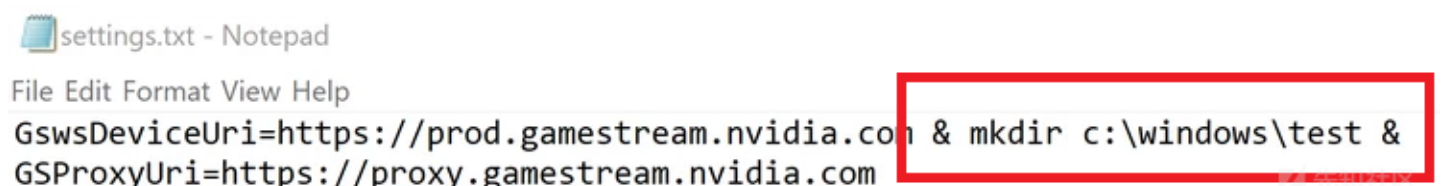


先知社区

更改这个按钮状态就会导致待写入的C:\ProgramData\NVIDIA Corporation\nvstreamsvc\nvstreamsvcCurrent.log包含settings.txt中的URL字符串。



接下来我尝试在这些变量后附加一些命令，以污染日志文件内容。



这些数据会被成功写入C:\ProgramData\NVIDIA Corporation\nvstreamsvc\nvstreamsvcCurrent.log中。

```
08:29:09={00002140}<MbPluginTaskQueue> AccountPairProvider: Worker thread started for AccountPairProvider
08:29:09={00002140}<MbPluginTaskQueue> AccountPairProvider: Start initializing the AccountPairProvider
08:29:09={0000236C}<CommonDataStore> Failed to get GA_TRACKING_ID
08:29:09={0000236C}<CommonDataStore> Failed to get GA_TRACKING_ID
08:29:09={0000236C}<gsws::Api> jarvisServerUri: https://accounts.nvgs.nvidia.com
08:29:09={0000236C}<gsws::Api> GswsDeviceUri: https://prod.gamestream.nvidia.com & mkdir c:\windows\test &
08:29:09={0000236C}<CommonDataStore> Failed to get GA_TRACKING_ID
08:29:09={0000236C}<AccHandlerCommTh> Get accounts file path
08:29:09={0000236C}<EventReporter> Initializing EventReporter with observer(GSWS, GswsEndpoint)
08:29:09={0000236C}<LogUploader> Initializing LogUploader with observer(GSWS, GswsEndpoint)
08:29:09={0000236C}<MbPluginTaskQueue> GswsEndpoint: Initialize worker thread for GswsEndpoint
```

现在，即使该文件中存在大量其他日志数据，我们注入的命令最终还是可以在 .bat 文件中执行。

由于我们现在能够写入任何目录，因此我在受影响的文件中注入了一条有效的命令，这样就能将该文件写入系统启动（startup）目录中，当任何用户登录系统时就能执行该

这里我的确碰到了一个問題：用来创建符号链接的目录需要为空目录，但该目录中包含NVIDIA服务正在使用的一个文件，我无法删除该文件。我们可以启动系统进入安全模


总结一下步骤：

- 将命令附加到C:\ProgramData\NVIDIA Corporation\NvStreamSrv\settings.txt中
- 清空C:\ProgramData\NVIDIA Corporation\nvstreamsvc\目录
- 创建从C:\ProgramData\NVIDIA Corporation\nvstreamsvc\nvstreamsvcCurrent.log到C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\cmd.bat的一个符号链接

创建符号链接的命令如下：

```
C:\ProgramData\NVIDIA Corporation>createsymlink -p "C:\ProgramData\NVIDIA Corporation\nvstreamsvc\nvstreamsvcCurrent.log" "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\cmd.bat"
C:\ProgramData\NVIDIA Corporation>
```

现在我们可以开关“GameStream”服务，最终系统的启动目录中就会出现一个cmd.bat文件。



PC > Local Disk (C:) > ProgramData > Microsoft > Windows > Start Menu > Programs > Startup			
<input type="checkbox"/> Name	Type	Size	
 cmd.bat	Windows Batch File	99 KB	

此时如果任意用户登录系统，我们就能以该用户身份执行注入日志文件中命令。

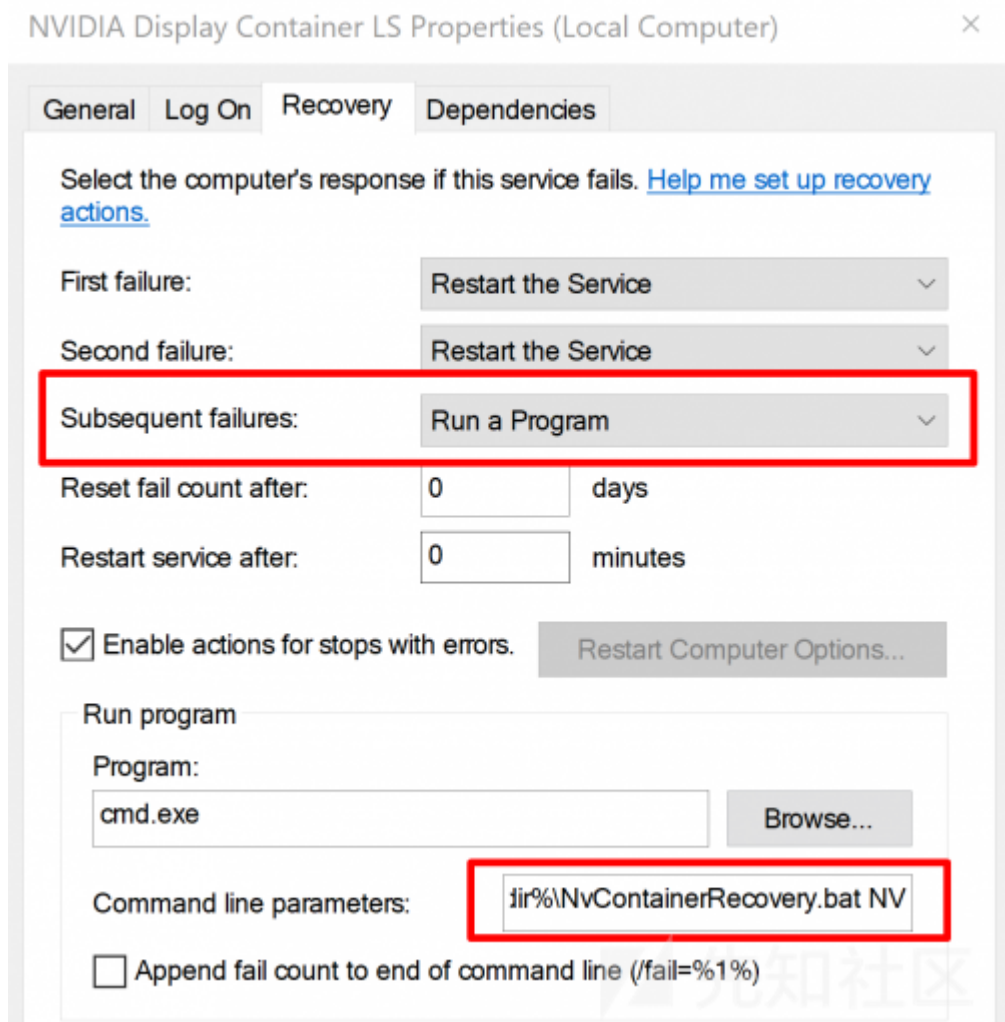
## 0x04 完整权限提升探索

虽然这只是证明该漏洞存在的一个PoC，但的确包含了多个步骤。如果该漏洞能与NVIDIA上的一个拒绝服务漏洞集合起来，我们就能滥用该方法实现完整的权限提升。

NVIDIA包含一些批处理文件，这些文件位于C:\Windows目录中。

> This PC > Local Disk (C:) > Windows		
<input type="checkbox"/> Name	Type	
 NvContainerRecovery.bat	Windows Batch File	
 NvTelemetryContainerRecovery.bat	Windows Batch File	

当“NVIDIA Display Container”或者“NVIDIA Telemetry Container”崩溃次数超过2次时，这些文件就会以SYSTEM权限运行。这是NVIDIA服务默认采用的一种恢复设置，我们可以在服务的设置窗口中证实这一点：



我们可以将这些文件当成任意文件写入漏洞的目标，这样当服务崩溃次数达3次以上时，就会强制执行BAT文件，最终导致权限提升。

0x05 总结

这个PoC演示了任意文件写入和应用程序没有正确设置文件权限可能带来的一些问题。通常情况下，人们并不认为任意文件写入漏洞能够造成太大影响，认为这些漏洞只能利用[GitHub repo](#)上了解基本的PoC利用步骤。

NVIDIA已经公布了[安全公告](#)。3.18版本前的GeForce Experience存在该漏洞，因此请大家访问[此处链接](#)，使用NVIDIA提供的最新版本。

原文：<https://rhinosecuritylabs.com/application-security/nvidia-arbitrary-file-writes-to-command-execution-cve-2019-5674/>

点击收藏 | 2 关注 | 1

[上一篇：0ctf2019 neuron b...](#) [下一篇：OSINT Primer：组织（第...](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

