



Oliver Schwarz  
oliver.schwarz@syss.de

DEEPSEC



# We are sorry that your mouse is admin

## Privilege escalation through the Razer co-installer



# ABOUT US



- SySS GmbH
- Pentesting, red teaming, seminars, incident response
- Since 1998
- Tübingen, Munich, Frankfurt, Vienna

# ABOUT US



- Dr. Oliver Schwarz
- Senior IT Security Consultant
- OSCP, GREM
- IT Security Consultant since 2018
- Academic researcher before that



- Dipl.-Inf. Matthias Deeg
- Senior Expert IT Security Consultant
- Head of Research & Development
- CISSP, CISA, OSCP, OSCE
- IT Security Consultant since 2007

# AGENDA



- Windows plug'n'play PrivEsc
- Demo on jonhat's attack
- Fake it until you make it
- Disclosure journey
- Insights on Windows access control
- Demo on our attack
- Related vulnerabilities
- Your future research



# THE SELECT PATH DIALOG BUG



# THE SELECT PATH DIALOG BUG



Demo time

# BASH BUNNY



PRODUCTS ▾ SHOWS PAYLOADS



COMMUNITY SUPPORT ▾

## BASH BUNNY

\$119.99

The groundbreaking payload platform that introduced multi-vector USB attacks has evolved.

Pull off covert attacks or IT automation tasks faster than ever with just the flick of a switch. The NEW Bash Bunny Mark II goes from plug to pwn in 7 seconds – so when the light turns green it's a hacked machine.

Now with **faster performance, wireless geofencing, remote triggers and MicroSD support**, the Bash Bunny is an even more impressive tool for your Red Team arsenal.

Simultaneously mimic multiple trusted devices to trick targets into divulging sensitive information without triggering defenses. The Bash Bunny is truly the world's most advanced USB attack platform.



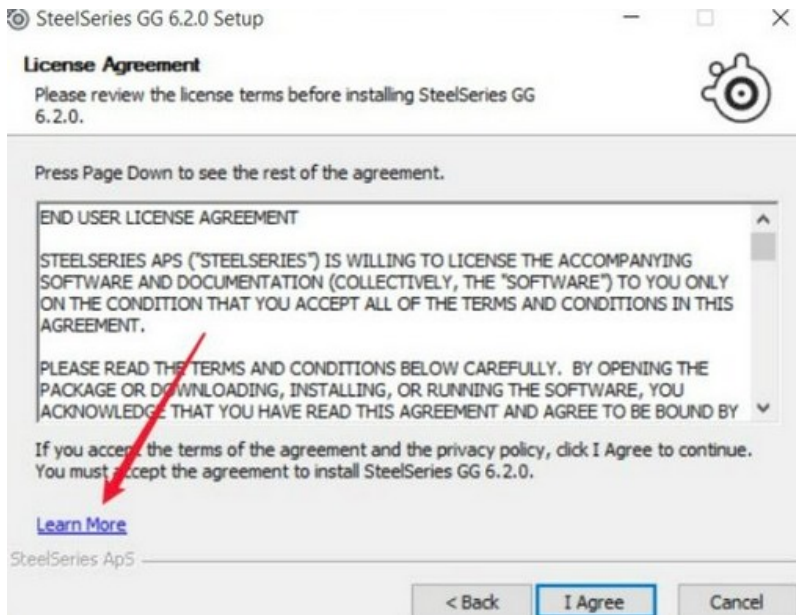
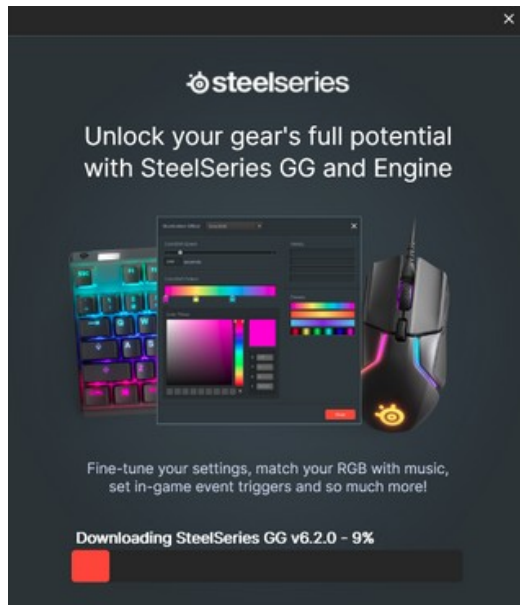
# EMULATING DEVICES

- Bash Bunny
- Raspberry Pi Zero
- Rooted Android
- OMG cable
- Vendor ID 0x1532 + Product ID 0x0084





# STEEL SERIES



0xsp SRD

Security Research & Development

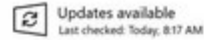


<https://0xsp.com/security%20research%20%20development%20srd/local-administrator-is-not-just-with-razer-it-is-possible-for-all/>

# MAGIC CONTROL TECHNOLOGY



## Windows Update



Updates available

Last checked: Today, 8:17 AM

Magic Control Technology Corporation - USB - 1.0.2301.615

Status: Pending install

Synaptics Incorporated - Biometric - 5.5.3534.1066

Status: Pending install



Will Dormann

@wdormann

Don't forget that some drivers may only show up via Windows Update, as opposed to automatically installing. We can still do this as a non-admin user, so no worries.

Here's an installer that popped up with SYSTEM privileges after reboot.



# LIVE HACKS



# DLL HIJACKING



File Explorer window showing the directory structure of CoolSoftware. The ribbon includes File, Home, Share, and View. The ribbon tabs are Clipboard, Organise, New, Open, and Select. The address bar shows the path: This PC > Local Disk (C:) > CoolSoftware. The file list contains:

Name	Date modified	Type	Size
program.exe	07/12/2019 10:09	Application	20 KB
userenv.dll	10/06/2022 22:50	Application exten...	17 KB

# C:\PROGRAMDATA



THE PENTEST  
EXPERTS.

← → ↕ ↑ This PC > Local Disk (C:) > ProgramData > Razer > Synapse3 > Service > bin >

Name	Date modified	Type	Size
Devices	18/09/2022 15:38	File folder	
AccountManagerClient.dll	17/08/2022 03:58	Application exten...	82 KB
AccountManagerCommon.dll	17/08/2022 03:58	Application exten...	99 KB
ActionServiceCommon.dll	17/08/2022 03:58	Application exten...	111 KB
BLEConnect.dll	10/06/2022 03:19	Application exten...	39 KB
BLEConnectWrapper.dll	10/06/2022 03:19	Application exten...	177 KB
BouncyCastle.Crypto.dll	17/08/2022 03:58	Application exten...	2.324 KB
Castle.Core.dll	29/08/2022 22:40	Application exten...	443 KB
Castle.Core.xml	04/04/2019 19:50	XML Document	419 KB
Common.Acceleration.dll	29/08/2022 22:40	Application exten...	15 KB
Common.Accessory.LedBrightness.dll	29/08/2022 22:40	Application exten...	16 KB
Common.Accessory.LedBrightness.xml	29/08/2022 21:26	XML Document	2 KB
Common.ApplicationEventsHandler.dll	29/08/2022 22:40	Application exten...	30 KB
Common.ApplicationLauncher.dll	29/08/2022 22:40	Application exten...	18 KB
Common.Audio.dll	29/08/2022 22:40	Application exten...	44 KB

# SYNAPSE 1.0.0 VULNERABILITY



```
Discovered by: Juan Sacco <jsacco@exploitpack.com>  
Razer Synapse Service v1.0.0 is prone to a DLL Injection because it  
fails to properly filter user supplied input and loads a .DLL from  
%ProgramData% from userland with SYSTEM rights allowing to escalate  
the privileges from a regular user to SYSTEM rights.
```

```
Program: Raze Synapse Service  
Version: 1.0.0  
Vendor: https://www.razer.com/  
Download link: https://www.razer.com/downloads
```

```
Steps To Reproduce:  
Move your .DLL to C:\ProgramData\Razer\Synapse3\Service\Bin\HID.dll  
Restart the PC or restart the service. The service runs with SYSTEM rights.  
Enjoy your privilege escalation!
```

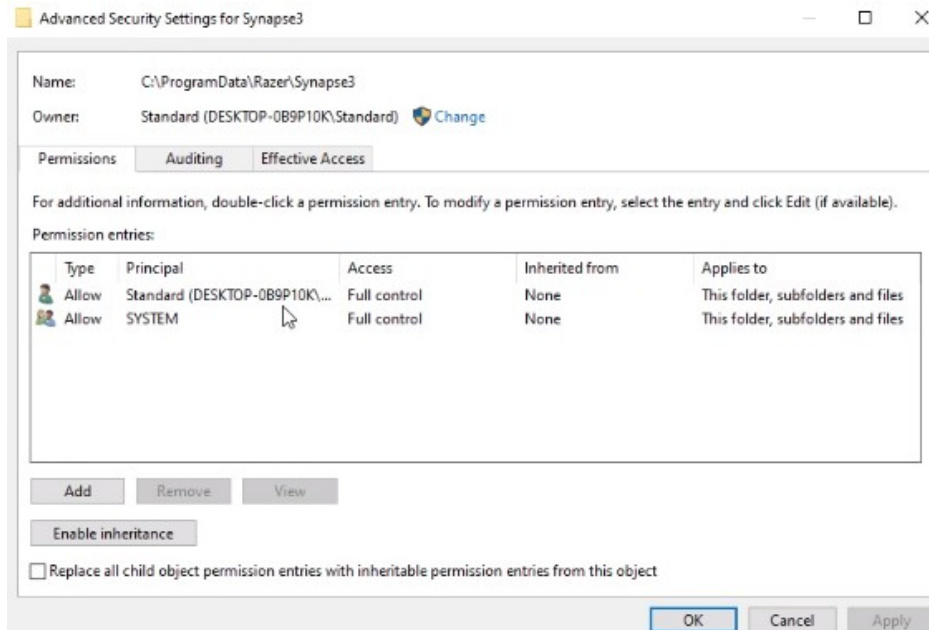
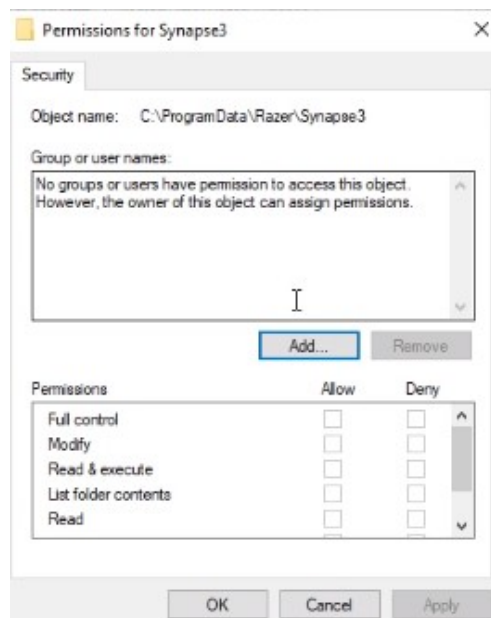
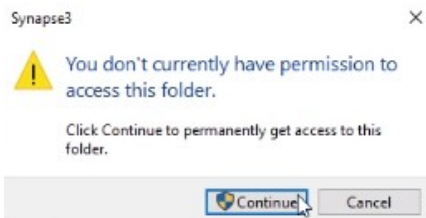
Discovered by Juan Sacco in 2003 (?)

<https://dl.packetstormsecurity.net/2003-exploits/razersynapse100-dllinject.txt>

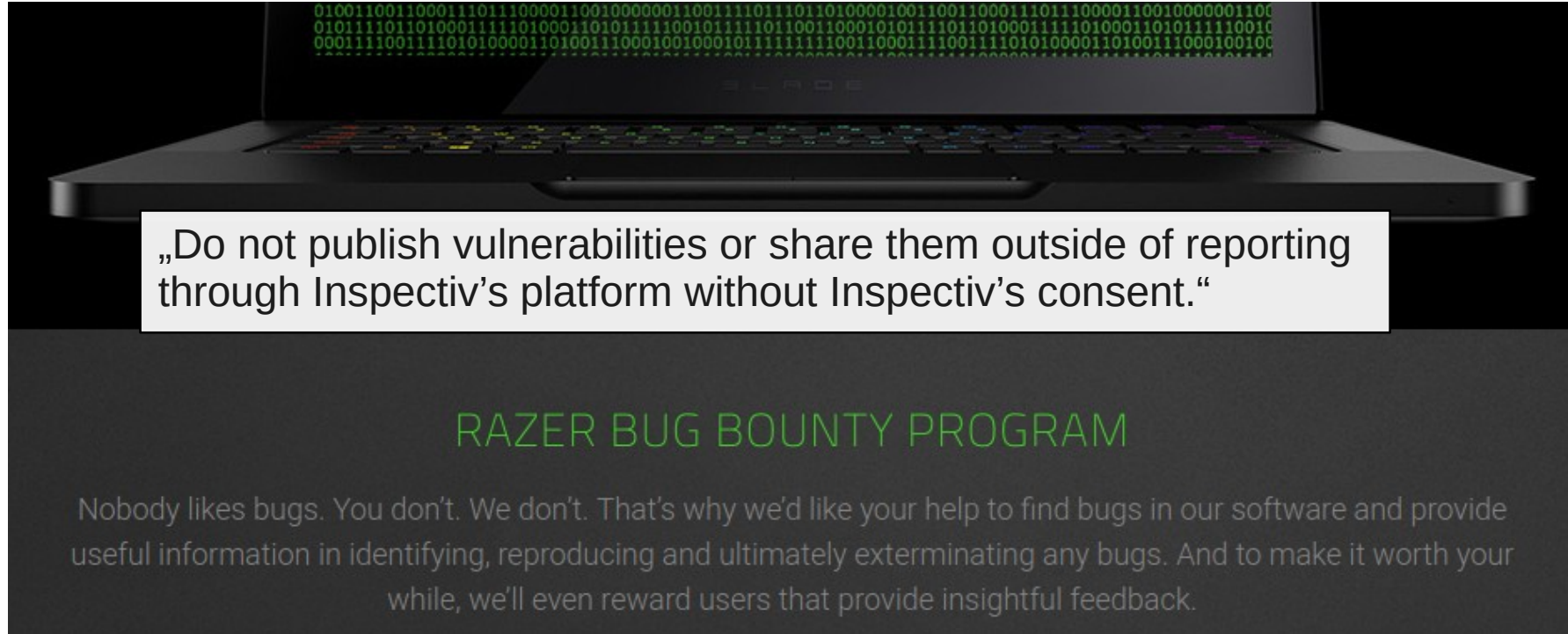
# INSIGHT 1



- If we are first to create the directory, we will remain owner
- CVE-2021-44226



# BUG BOUNTY VS. RESPONSIBLE DISCLOSURE







# DISCLOSURE JOURNEY



we have already submitted the fix to Microsoft and is currently in the "Gradual Rollout" phase

Oct 12

Thank you so much for bringing this issue to our attention. [...] We appreciate your feedback on our Razer Synapse application. This request will be recorded and will be forwarded to our Feature Request Poll.

Oct 19

We discovered something

Oct 11

OK, here some details

Oct 18



# DISCLOSURE JOURNEY



We will endorse your case to the relevant team who can handle your concern.

Nov 25

We have not heard back from you.

Nov 27

We have not heard back from you.

Nov 29

Any update?

Nov 25



# DISCLOSURE JOURNEY



I understand that your Razer Synapse has Elevated Admin access. We do apologize for the inconvenience that this has caused you. This is not the experience that we would like you to have.

Dec 2

This is confirmed to be a false alert, Razer is working with Windows Defender Team to prevent this in future Windows Defender Updates.

Dec 11

No!

Dec 12



# DISCLOSURE JOURNEY



we have already submitted the fix to Microsoft and is currently in the "Gradual Rollout" phase

Dec 13

While I understand the process has been slow so far, we take security matters very seriously and we appreciate your findings. [...]  
I'll be happy to answer either in english or german!

Dec 31

Here is the contact to the developers...

Jan 18

# CVE-2021-44226



Demo time

# INSIGHT 2

- We remain owner
- As creator we keep some privileges along the path
- Ownership of sub-directories doesn't matter much
- We can simply rename parent directories



# INSIGHT 3

- We remain owner
- As creator we keep some privileges along the path
- Ownership of sub-directories doesn't matter much
- We can simply rename parent directories
- Even SYSTEM can be locked out



# SOLUTION MARCH 2022



→ Don't start service if foreign DLLs are found and cannot be deleted



# CLOSER LOOK 3 MONTHS LATER



→ Don't start service if foreign DLLs are found and cannot be deleted

```
try
{
    X509Certificate2 x509Certificate = new X509Certificate2(X509Certificate.CreateFromCertFile(text));
}
catch (CryptographicException ex)
{
    string text2 = string.Format("File {0} is not signed. Skipping due to security concerns.", text);
    service.EventLog.WriteEntry(text2, EventLogEntryType.Error);
    Trace.TraceError(text2, new object[]
    {
        ex
    });
    if (!hashSet.Contains(text))
    {
        hashSet.Add(text);
    }
}
```

# SYNAPSE 3.3 VULNERABILITY



```
List<Assembly> list = new List<Assembly>();
X509Certificate2 x509Certificate = new X509Certificate2(X509Certificate.CreateFromCertFile(Path.Combine
(AppDomain.CurrentDomain.BaseDirectory, "razer.cer")));
foreach (string text2 in Directory.GetFiles(text, "*.dll", SearchOption.AllDirectories))
{
    try
    {
        bool flag = false;
        X509Certificate2 x509Certificate2 = new X509Certificate2(X509Certificate.CreateFromSignedFile(text2));
        if (x509Certificate != null && x509Certificate2 != null)
        {
            flag = x509Certificate.Equals(x509Certificate2);
        }
        if (!flag)
        {
            Trace.TraceInformation(string.Format("{0} is not verified razer assembly!. Aborting.", text2));
        }
    }
}
```

Discovered by enigma0x3 (Matt N.) in 2018

<https://enigma0x3.net/2019/01/21/razer-synapse-3-elevation-of-privilege/>

# SYNAPSE 3.3 VULNERABILITY (FIX)



```
List<Assembly> list = new List<Assembly>();
X509Certificate2 x509Certificate = new X509Certificate2(X509Certificate.CreateFromCertFile(Path.Combine(AppDomain.CurrentDomain.BaseDirectory, "razer.cer")));
foreach (string text2 in Directory.GetFiles(text, "*.dll", SearchOption.AllDirectories))
{
    try
    {
        if (!WinTrust.VerifyEmbeddedSignature(text2))
        {
            Trace.TraceInformation(string.Format("{0} is not trusted!. Aborting.", text2));
        }
        else
        {
```

Discovered by enigma0x3 (Matt N.) in 2018

<https://enigma0x3.net/2019/01/21/razer-synapse-3-elevation-of-privilege/>

# SYNAPSE 3.3 VULNERABILITY (TIMELINE)



**06/05/2018:** Submitted vulnerability report to Razer's HackerOne program  
**06/08/2018:** Response posted on the H1 thread acknowledging the report  
**06/08/2018:** H1 staff asked for specific version number of the Synapse 3 installer  
**06/08/2018:** Synapse 3 installer version number provided to Razer  
**07/05/2018:** Asked for an update  
**08/06/2018:** Report marked as triaged  
**08/27/2018:** Asked for an update, no response

**12/25/2018:** I was contacted by someone at Razer with a link to an internal build for remediation verification  
**12/27/2018:** Per their request, provided feedback on the implemented mitigation via the H1 report  
**01/09/2019:** Asked for a timeline update for the fixed build to be provided to the public (via H1)  
**01/10/2019:** Informed that the build is now available to the public

Discovered by `enigma0x3` (Matt N.) in 2018

<https://enigma0x3.net/2019/01/21/razer-synapse-3-elevation-of-privilege/>

# SOLUTION SEPTEMBER 2022



```
try
{
    X509Certificate2 x509Certificate = new X509Certificate2(X509Certificate.CreateFromCertFile(text));
    FileInspector fileInspector = new FileInspector(text);
    if (fileInspector != null)
    {
        SignatureCheckResult signatureCheckResult = fileInspector.Validate(RevocationChecking.Offline);
        if (signatureCheckResult != SignatureCheckResult.Valid)
            // mark evil
    }
}
catch (CryptographicException ex)
{
    // mark evil
}
catch (Exception arg)
{
    Trace.TraceError(string.Format("{0}: {1}", text, arg));
}
```

# LESSONS FOR DEVELOPERS

- Be aware of DLL injection
- Mind owners and creators
- Check access control also for SYSTEM
- „C:\Program Files“ is your friend



# LESSONS FOR ADMINS



- Prevent Device-Specific Co-Installers
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Device Installer\DisableCoInstallers = 1
- Control USB devices
- Also, careful with directory access rights

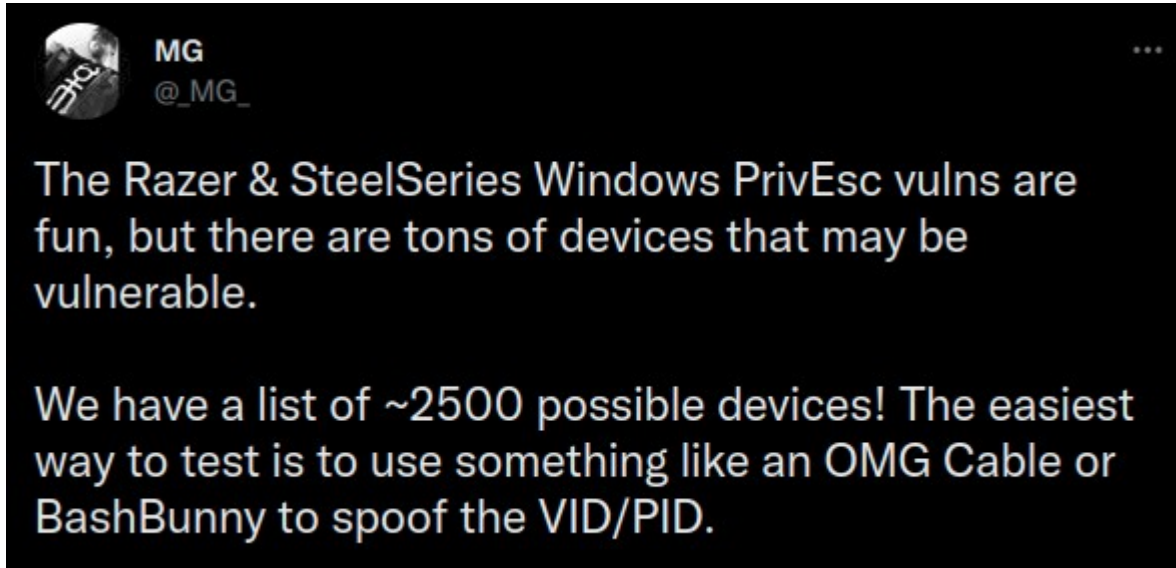
# LESSONS FOR RESEARCHERS

→ Co-Installers are a promising field





# FUTURE RESEARCH



# FUTURE RESEARCH



Tavis Ormandy ✓

@tavis0

Antwort an @tavis0 und @wdormann

There were around 10k unique drivers, but many were very minor product variations. Filtering those for unique command lines, there's only 298, that seems more manageable. Here's the output:

[lock.cmpxchg8b.com/files/coinstal...](https://lock.cmpxchg8b.com/files/coinstal...)

```
name '*.inf' -print0 | xargs -n1 -0 q  
[print $1}' coininstallers.txt | xargs  
;.zip | tail
```

```
95_1669f3be7942815486b8c60e8a9a85216ec9256a/RealSenseR200I  
420_130c82a329bd45f0027bcd5e0629218c8f321875/RealSenseR200I  
23_ba292407b0691975e8705263da61cbe3458c4880/RealSenseF200I  
37_347f0f56514e537c3d41be1ffe0b398e6e871f8a/RealSenseSR300I  
76_0ab165512bab04f25ae2f7d9e23d675874b9ac4a/RealSenseSR300I  
98_0242f678b562bb5de426b4db9f71f93d5ec42be0/RealSenseR200I  
bd-fe23-4af1-ace6-529b6d1b5088_1e45bf7e97d3b26af466c9ae32f  
37 adb65b5271e3433d7577ac75ec325590801621d7/MosUPort.inf
```

# THANK YOU!



**Oliver Schwarz**  
oliver.schwarz@syss.de



# REFERENCES



- <https://enigma0x3.net/2019/01/21/razer-synapse-3-elevation-of-privilege/>
- <https://packetstormsecurity.com/files/156800/Razer-Synapse-Service-1.0.0-DLL-Injection.html>
- <https://www.youtube.com/watch?v=P75BtYcnZ-A>
- <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-058.txt>
- <https://blog.syss.com/posts/razer-lpe-attack/>