Shuttling Through Secret Pipes:

Unveiling Vulnerabilities in Leading VPNs

Zeze@ROOTCON

TEAMT5
杜 浦 數 位 安 全
Persistent Cyber Threat Hunters

Zeze

- TeamT5 Research Engineer
- HITCON Staff
- 2023~2024 DEFCON CTF Final
- CODE BLUE, HITCON, VXCON, CYBERSEC, SITCON Speaker

Outline

TEAMT5
杜 浦 數 位 安 全

- **Introduction** to named pipe and the target vendors
- **Background** of named pipe and how it works
- **Related Work** including the research, tools, and previous CVE
- **Method** I use to research on named pipe by creating a tool
- **Vulnerabilities** found in 3 VPNs
- **Fix** for the vulnerabilities
- **Report** submitted to each vendor and the timeline

Introduction

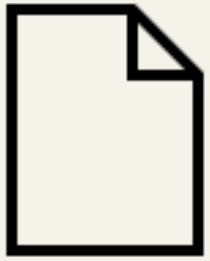
Introduction to named pipe and the target vendors

Named Pipe

TEAMT5
杜 浦 數 位 安 全

Introduced in Windows NT 3.1

Inter-Process Communication



FILE_OBJECT

Managed by NPFS

Windscribe

TEAMT5
杜 浦 數 位 安 全

Windscribe is a desktop application and browser extension that work together to block ads and trackers, restore access to blocked content and help you safeguard your privacy online.

- Written in **C/C++**
- Official Website - [Windscribe]
- An **open source** VPN - [Windscribe/Desktop-App]

CyberGhost

TEAMT5
杜 浦 數 位 安 全

CyberGhost is the VPN service in 2024. With 11712 servers, it offers top privacy for all devices, Windows, iOS, Mac, Android, or Linux.

- Written in **C#**
- Official Website - CyberGhost
- a **closed source** VPN

OpenVPN

TEAMT5
杜 浦 數 位 安 全

OpenVPN is a network security company serving the secure remote access needs of small businesses to the enterprise. Our on-prem and cloud-based products offer the essentials of zero trust network access and are built on the leading OpenVPN tunneling protocol.

- Written in **C**
- Official Website - OpenVPN
- An **open source** VPN - OpenVPN Inc

Achievement

TEAMT5
杜 浦 數 位 安 全

- v2.10.10 changelog.txt
- v2.10.12 changelog.txt
- CVE-2024-6141

- **bug bounty** report

  (but internally tested)

- CVE-2024-4877

What You Will Learn

TEAMT5
杜 浦 數 位 安 全

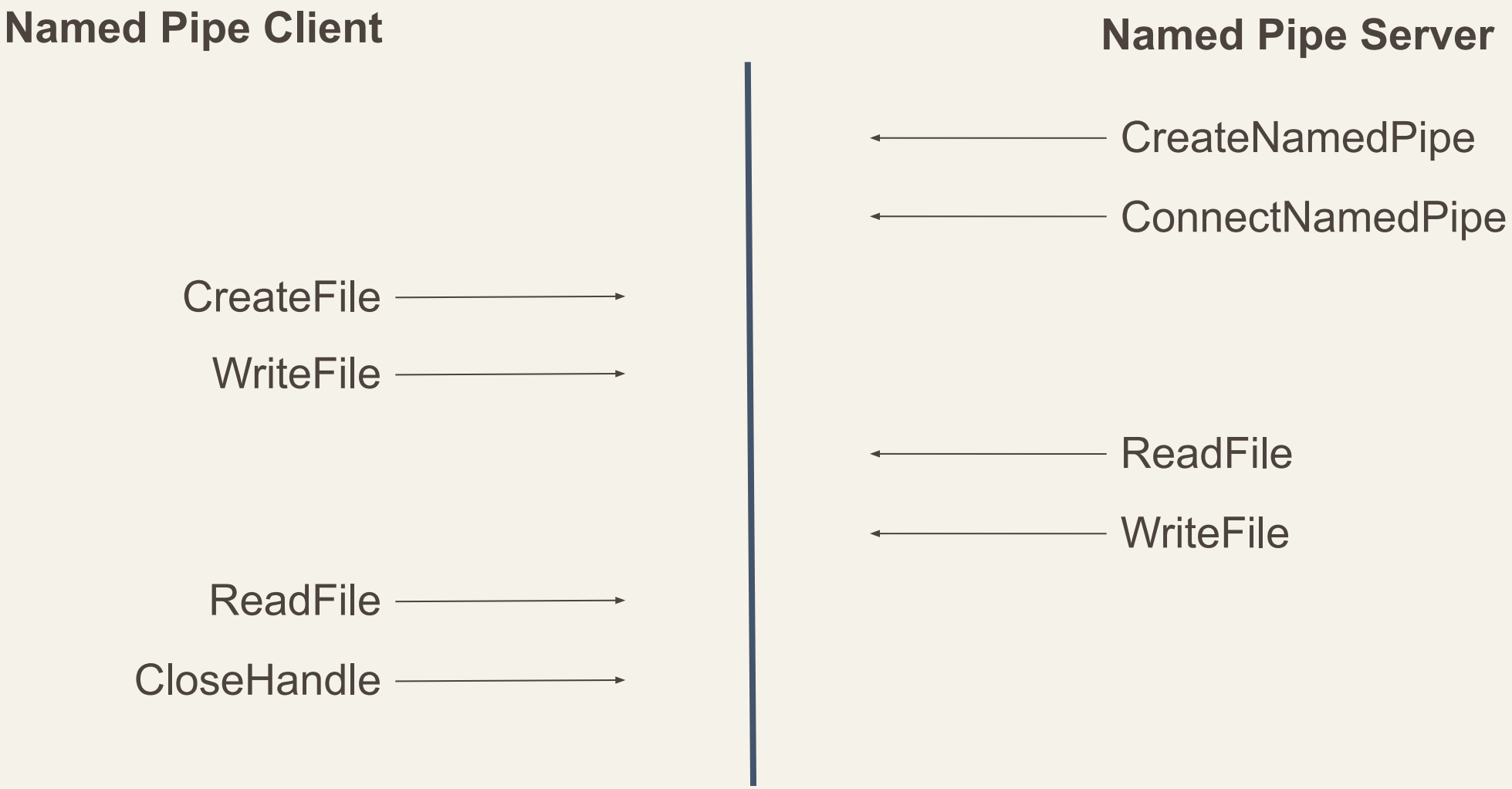
How named pipe works and related vulnerability types.

Impersonation in named pipe and secure implementation.

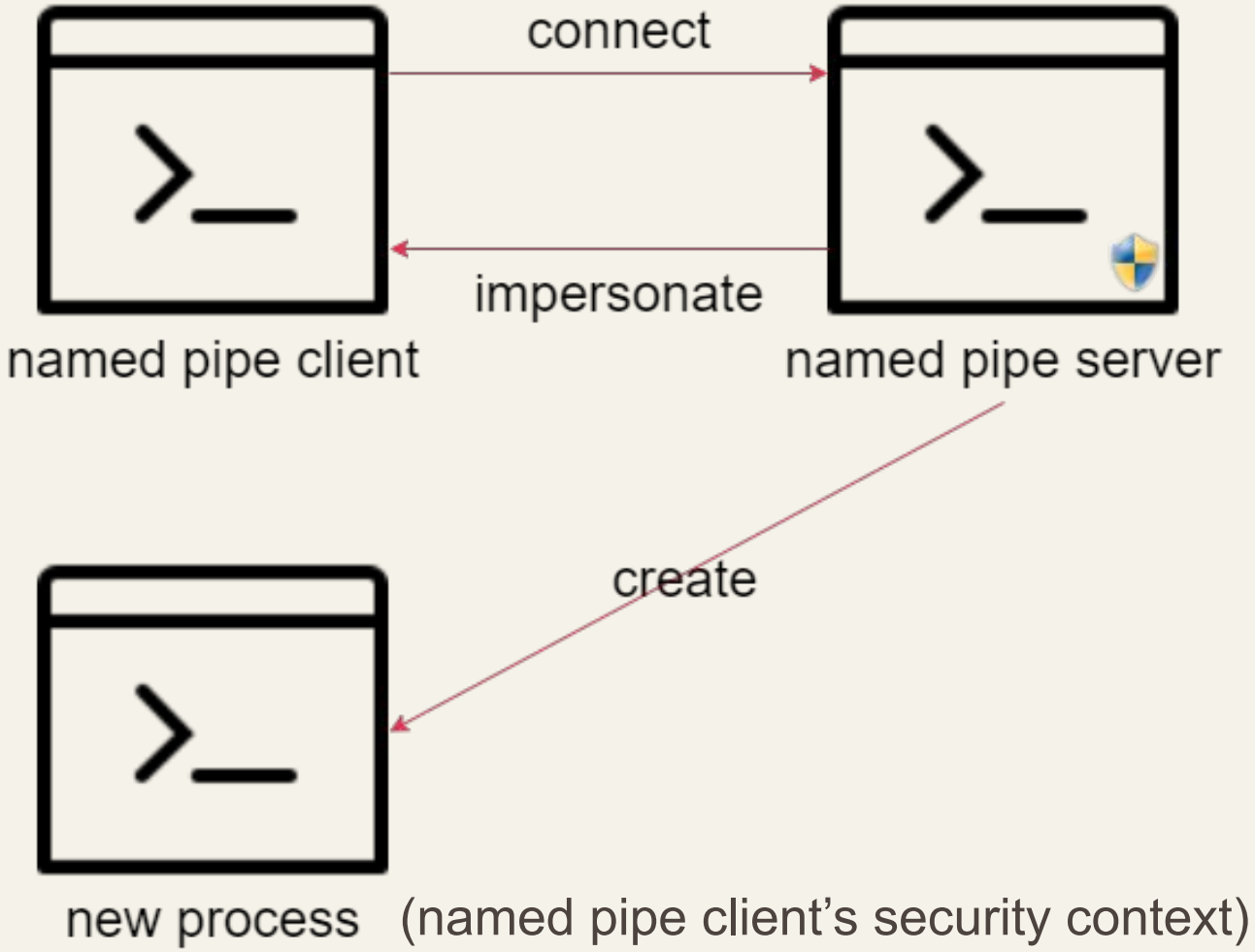
Background

Background of named pipe and how it works

Named Pipe Communication



Impersonation



SECURITY_IMPERSONATION

TEAMT5 杜浦數位安全

Named pipe server can impersonate if **SECURITY_IMPERSONATION** is set by named pipe client.

```
HANDLE CreateFileA(
  [in] LPCSTR lpFileName,
  [in] DWORD dwDesiredAccess,
  [in] DWORD dwShareMode,
  [in, optional] LPSECURITY_ATTRIBUTES lpSecurityAttributes,
  [in] DWORD dwCreationDisposition,
  [in] DWORD dwFlagsAndAttributes,
  [in, optional] HANDLE hTemplateFile
);
```

Impersonation Level

TEAMT5 杜浦數位安全

Low

High

SECURITY_IMPERSONATION_LEVEL	Identification	Impersonate
SecurityAnonymous	✗	✗
SecurityIdentification	○	✗
SecurityImpersonation	○	○ (only local)
SecurityDelegation	○	○ (local and remote)

ImpersonateNamedPipeClient

A caller can impersonate named pipe client if having the **SeImpersonatePrivilege**.

```
BOOL ImpersonateNamedPipeClient(
  [in] HANDLE hNamedPipe
);
```

SeImpersonatePrivilege

TEAMT5
杜 浦 數 位 安 全

Groups having SeImpersonatePrivilege by default

- Administrators
- Local Service
- Network Service
- IIS AppPool Account
- Microsoft SQL Server Account
- Service

Related Work

Related Work including the research, tools, and previous CVE

Why I Started This Research

TEAMT5 杜浦數位安全

Mandarin | Red | Exploit Development

Endpoint Security or End of Security? Exploiting Trend Micro Apex One

Instant Q&A

R0
Site

14:00 – 14:40
Sat, Aug 19

Talk
Type

EDR as a tool designed to enhance enterprise information security, could potentially become a security threat if improperly designed. In this session, we will share our methods of abusing the implementation issues in Trend Micro Apex One EDR to achieve local privilege escalation. Our research is focus on the IPC mechanism between the Security Agent and System Service of Apex One, encompassing both architectural design and implementation issues. In the process, we discovered and reported over ten local privilege escalation vulnerabilities, and even after these vulnerabilities were patched, we could still find new bypass techniques. In this session, we will delve into the architectural issues of Apex One and the evolution of its IPC authentication mechanism, as well as the root causes and exploitation methods of these vulnerabilities. Through this discussion, we hope to enable developers to gain a deeper understanding of the security issues that may be encountered in system services and to be more rigorous when developing information security products.

Lays

Shih-Fong Peng, aka Lays, is Co-Founder and Security Researcher of TRAPA Security, currently focusing on reverse engineering and vulnerability research. He is a member of HITCON and 217 CTF team which achieved second place at DEF CON CTF 25 and 27. He is also one of the 2019, 2020 MSRC Most Valuable Security Researcher and has reported vulnerabilities to Microsoft, Google, Samsung, etc.

Blog: https://blog.l4ys.tw Twitter: @_L4ys

Lynn

Lynn is a member of the iCYBER Advisor Security Team. She has successfully discovered and reported multiple vulnerabilities. Moreover, she was a member of the Balsn CTF team. Twitter: @0x000050

Known Tools

TEAMT5 杜浦數位安全

[pipelist64.exe]

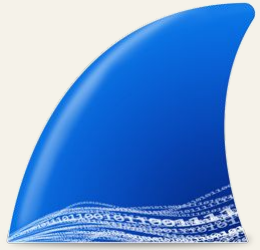
List named pipes.

[accesschk64.exe]

Check the ACL of a named pipe.

[Procexp64.exe]

Get named pipe handles in a process.



[Wireshark]

Observe named pipe through SMB.

Previous CVEs - Windscribe

TEAMT5 杜浦數位安全

- CVE-2018-11334: Windscribe 1.81 creates a named pipe with a **NULL DACL** that allows Everyone users to **gain privileges** or cause a **denial of service** via \\.\pipe\WindscribeService.
- CVE-2018-11479: The VPN component in Windscribe 1.81 uses the OpenVPN client for connections. Also, it creates a WindScribeService.exe system process that establishes a \\.\pipe\WindscribeService named pipe endpoint that allows the Windscribe VPN process to connect and execute an OpenVPN process or other processes (like taskkill, etc.). There is **no validation** of the program name before **constructing the lpCommandLine argument** for a CreateProcess call. An attacker can **run any malicious process with SYSTEM** privileges through this named pipe.

Previous CVEs - CyberGhost

TEAMT5 杜浦數位安全

- CVE-2023-30237: CyberGhostVPN Windows Client before v8.3.10.10015 was discovered to contain a **DLL injection vulnerability** via the component Dashboard.exe.
- Bullied by Bugcrowd over Kape CyberGhost disclosure: A specially **crafted JSON payload** sent to the CyberGhost RPC service can lead to **command line injection** when the OpenVPN process is launched, leading to full system compromise.

Previous CVEs - OpenVPN

TEAMT5 杜浦數位安全

- CVE-2024-27459: When reading message from the pipe, we first peek the pipe to get the size of the message waiting to be read and then read the message. A compromised OpenVPN process could send an excessively large message, which would result in a **stack-allocated message buffer overflow**.
- CVE-2024-24974: If an attacker manages to get credentials for a user which is the member of "OpenVPN Administrators" group on a victim machine, an attacker might be able to communicate with the privileged interactive service on a victim machine and **start openvpn processes remotely**.

Method

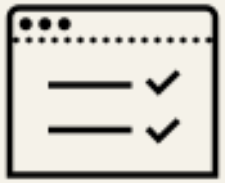
Method I use to research on named pipe by creating a tool

Difficulties

TEAMT5
杜 浦 數 位 安 全

Where does the program **read/write** named pipe buffer?

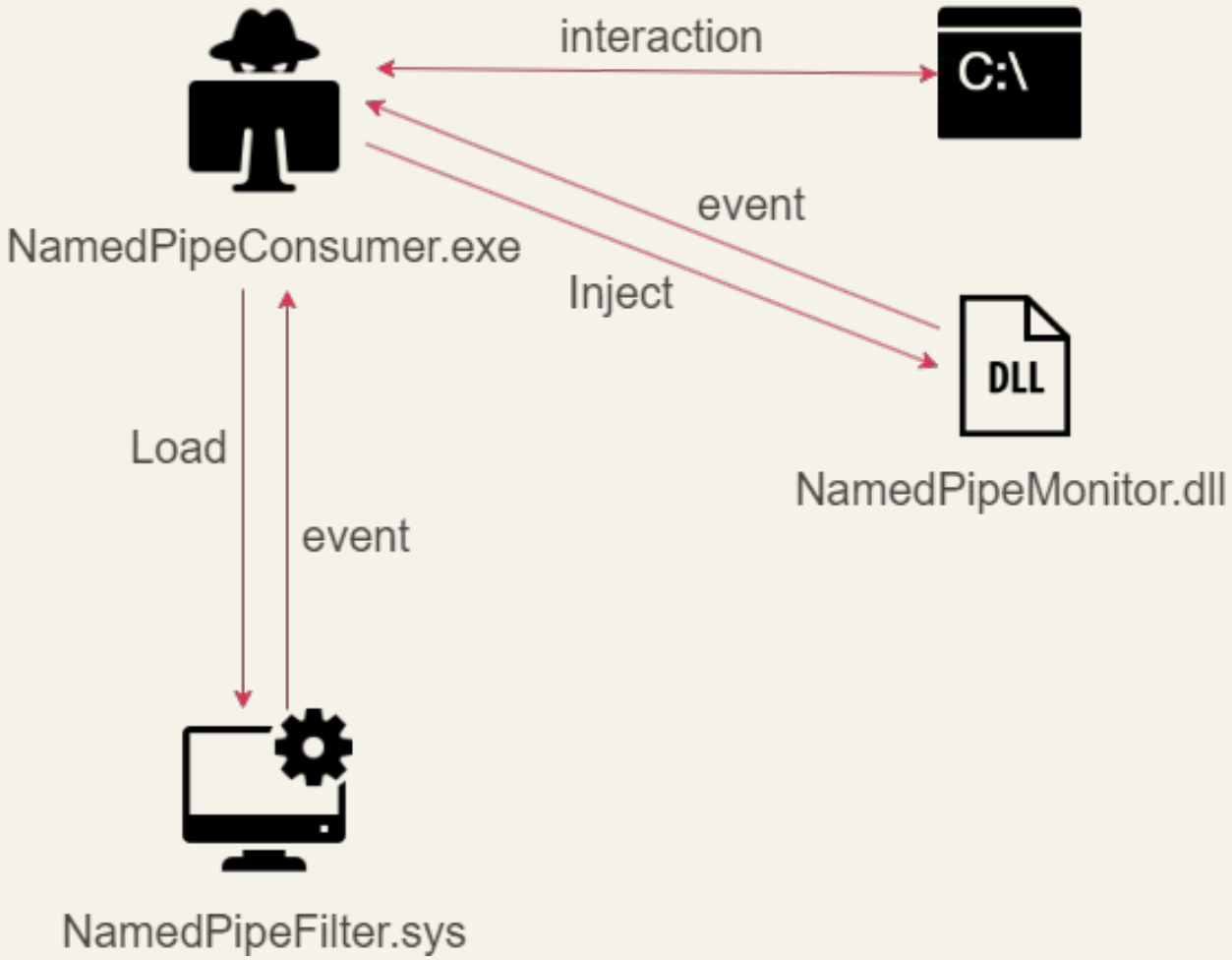
How to **bypass** the **image check** from named pipe server **efficiently**?



How to test **impersonation** vulnerability **automatically**?

NamedPipeMaster

TEAMT5
杜 浦 數 位 安 全

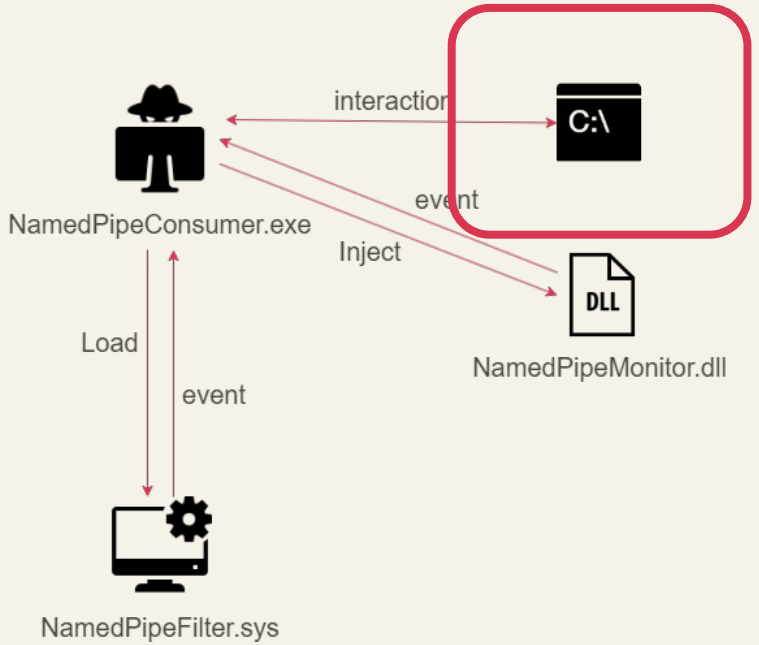


NamedPipeMaster

TEAMT5
杜 浦 數 位 安 全

Interact with a named pipe server/client.

- **Proactively interact** with a named pipe server.
- **Passively connected** by a named pipe client.
- **Inject dll** into a process as a proxy.

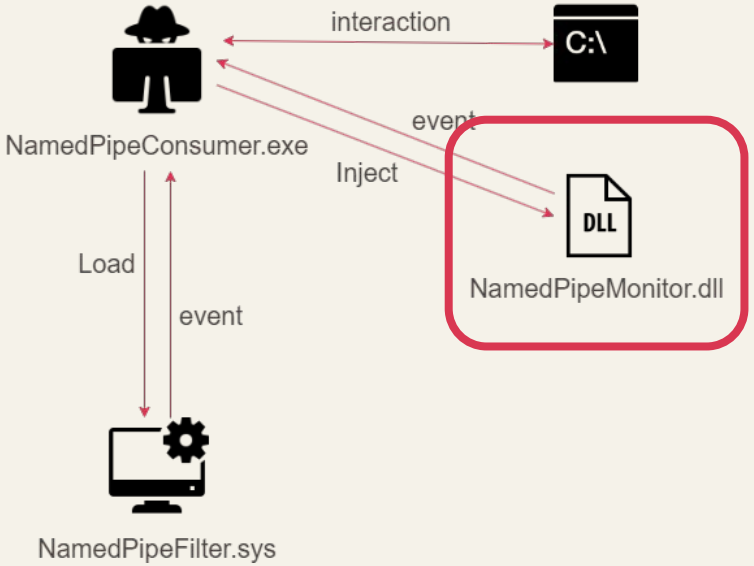


NamedPipeMaster

TEAMT5 杜浦數位安全

Collect named pipe communication with **ring3 hook** by **dll injection**.

- NtCreateNamedPipeFile: named pipe created
- NtCreateFile: connect named pipe
- NtFsControlFile: named pipe connected
- NtReadFile: read data from named pipe
- NtWriteFile: write data to named pipe

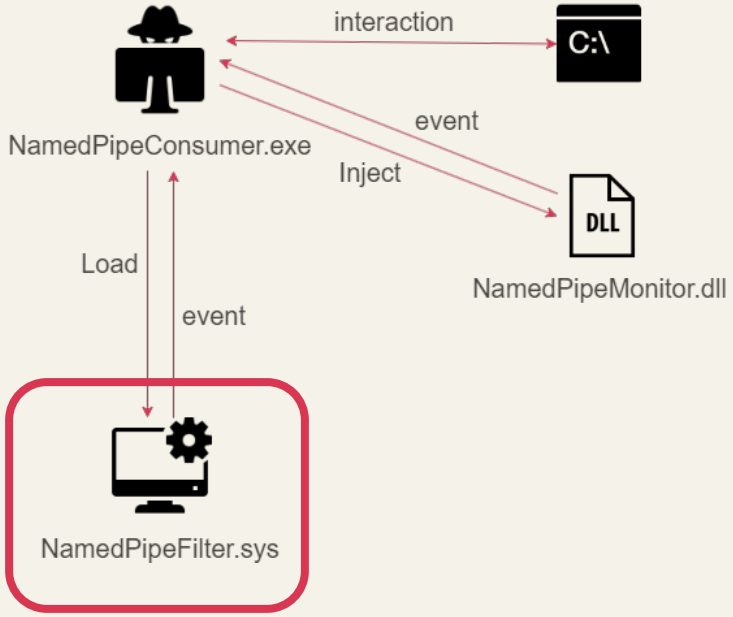


NamedPipeMaster

TEAMT5 杜浦數位安全

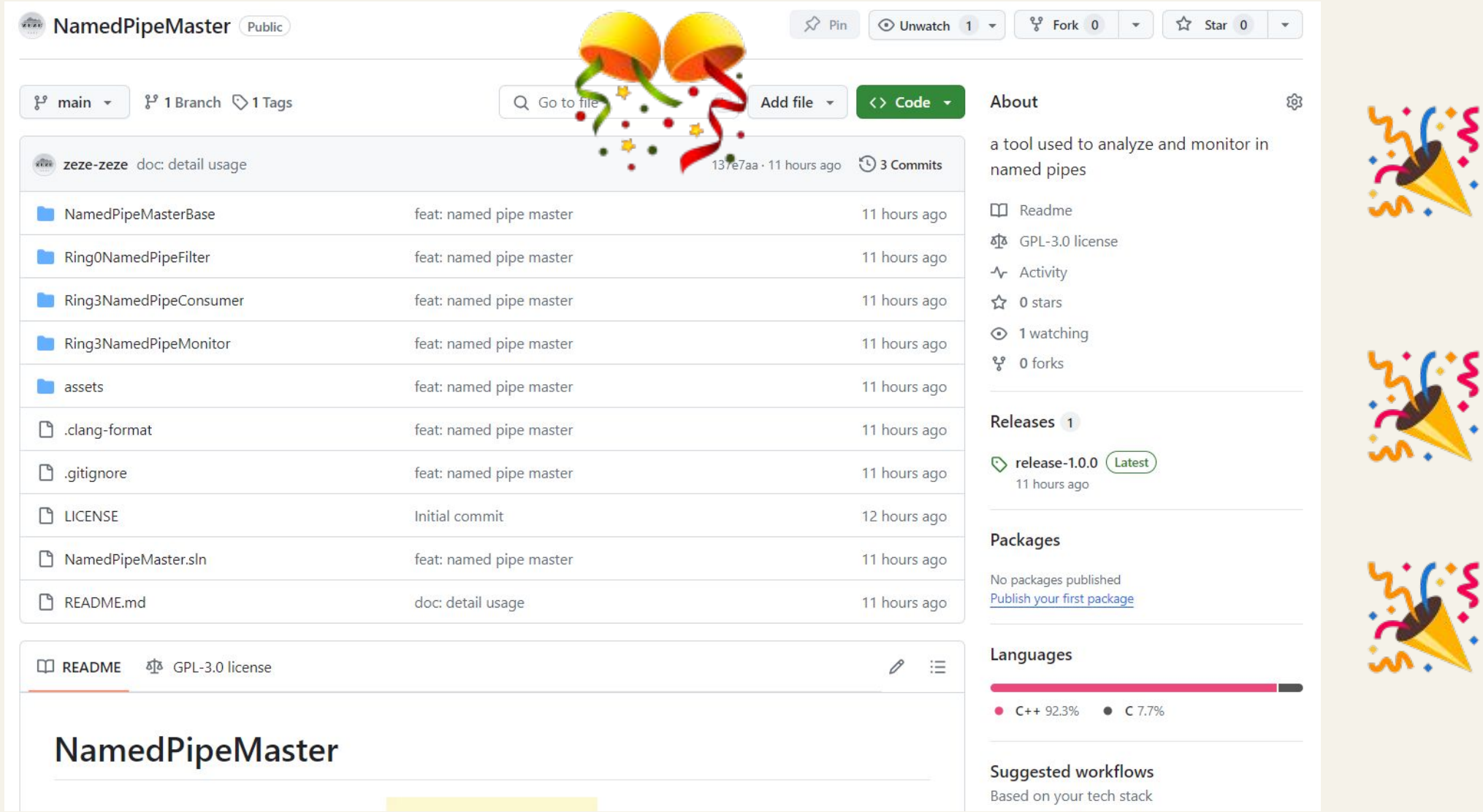
Collect named pipe information with **minifilter driver**

- IRP_MJ_CREATE_NAMED_PIPE: named pipe created
- IRP_MJ_CREATE: connect named pipe
- IRP_MJ_FILE_SYSTEM_CONTROL: named pipe connected
- IRP_MJ_READ: read data from named pipe
- IRP_MJ_WRITE: write data to named pipe



NamedPipeMaster

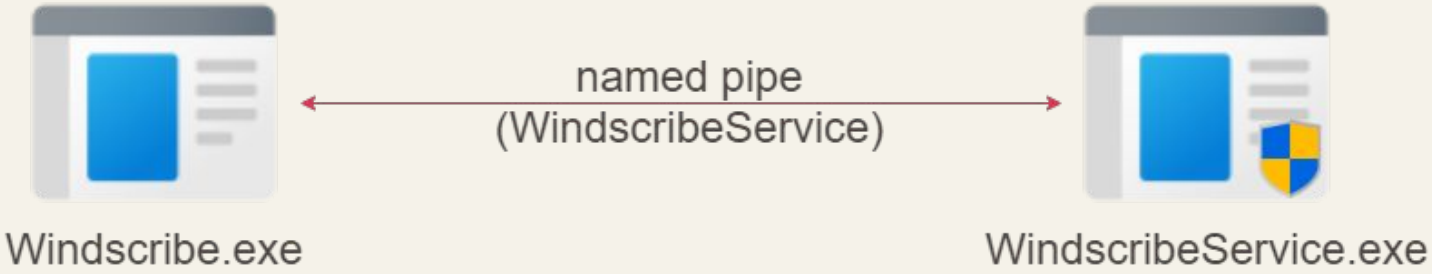
TEAMT5 杜浦數位安全



Vulnerabilities

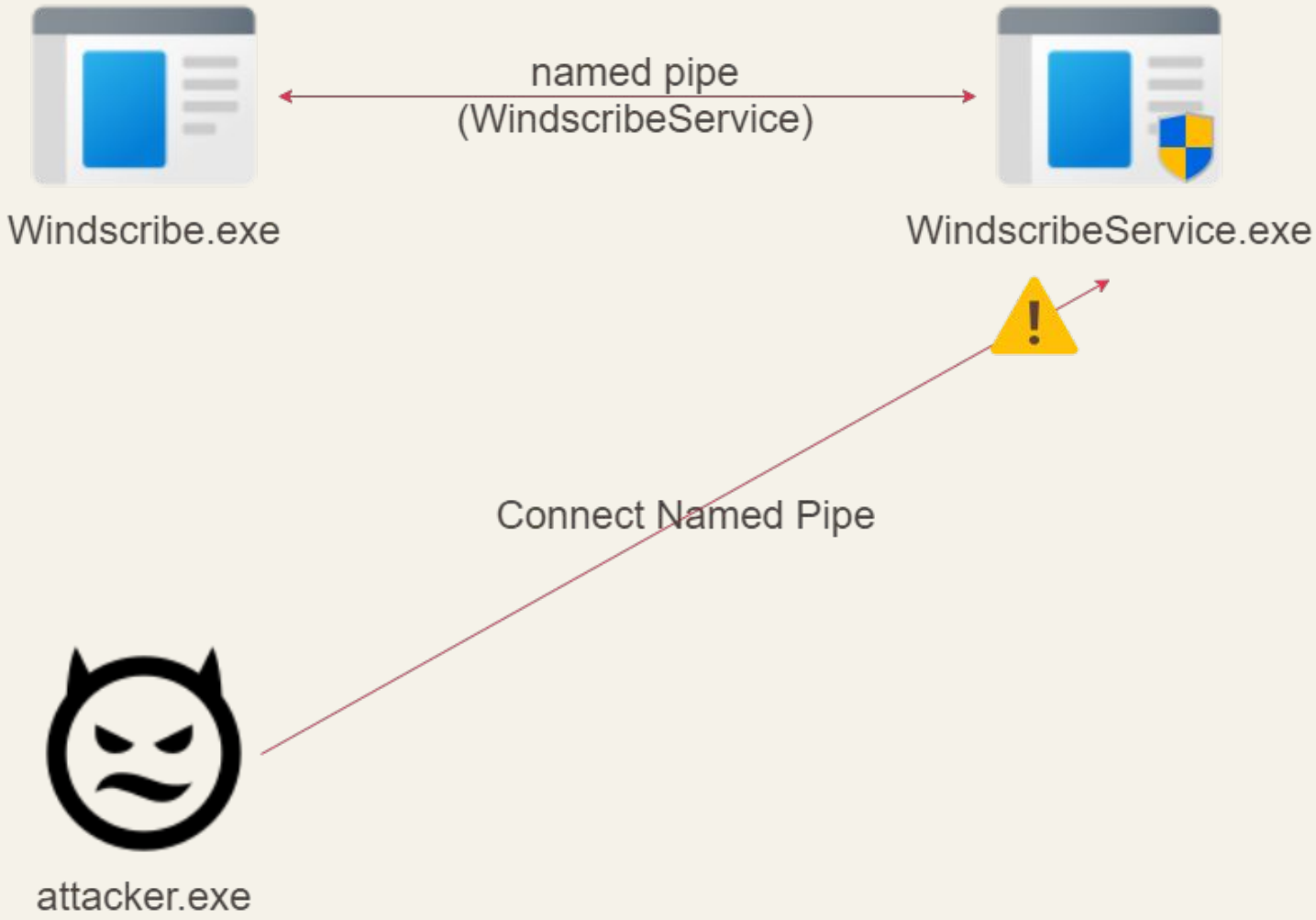
Vulnerabilities found in 3 VPNs

Windscribe Vulns

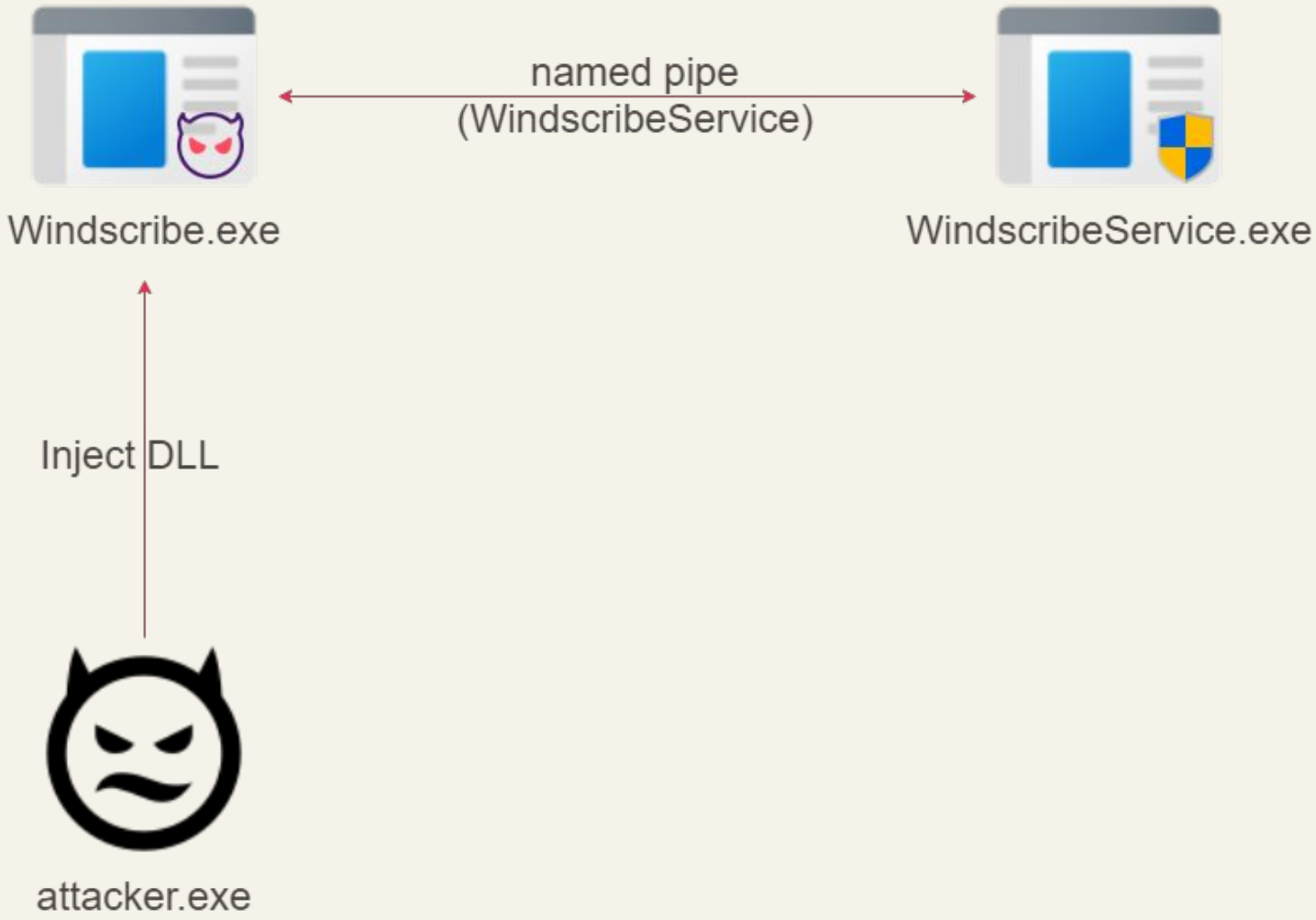



```
\\.\Pipe\WindscribeService
  RW BUILTIN\Guests
  RW NT AUTHORITY\Authenticated Users
  RW BUILTIN\Administrators
```

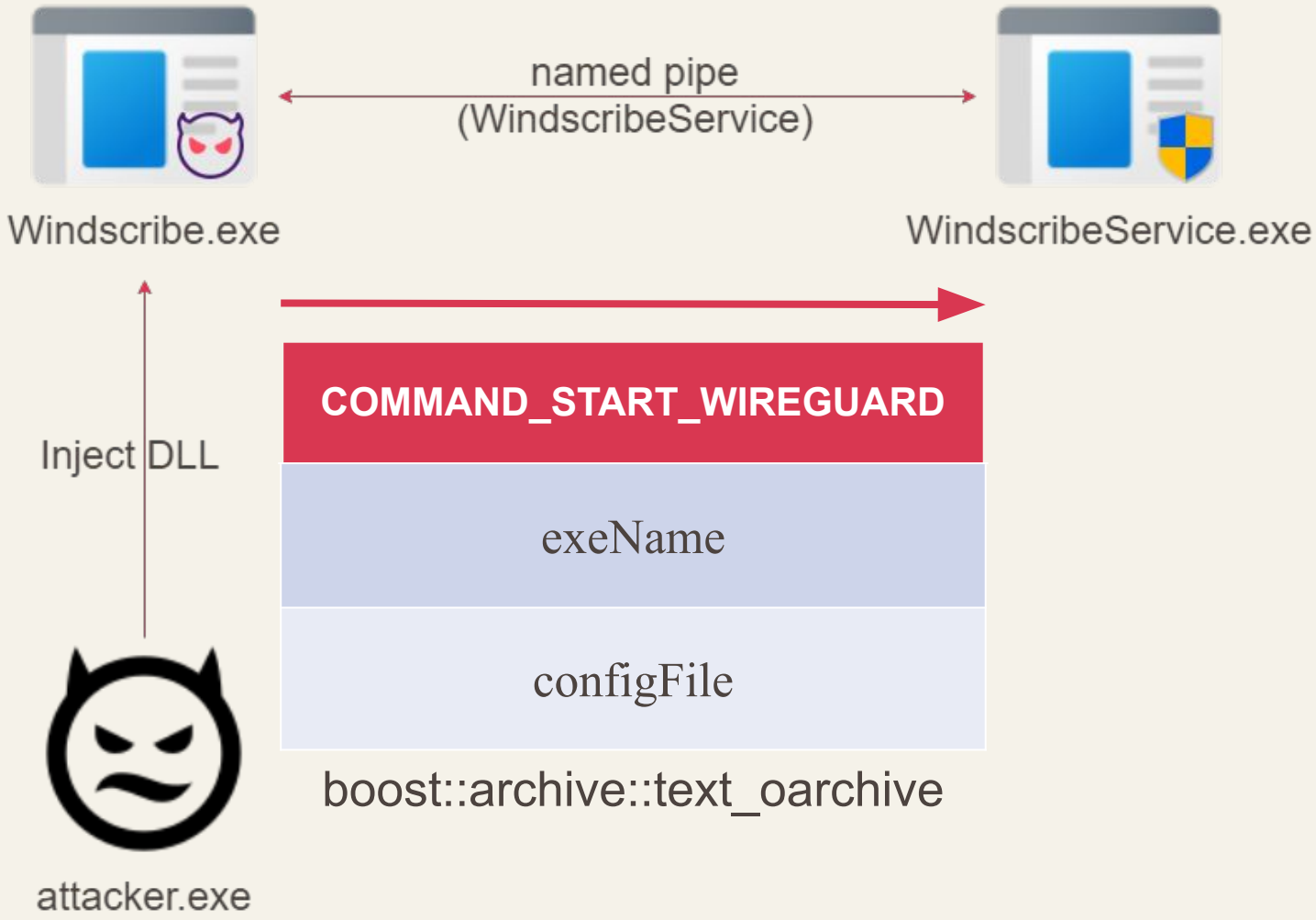
Image Check


named pipe
(WindscribeService)
Windscribe.exe
WindscribeService.exe
Connect Named Pipe
attacker.exe

Bypass Image Check



Windscribe VuIn1



Windscribe VuIn1

AA_COMMAND_START_WIREGUARD: An authenticated user or guest can exploit the vulnerability to **run arbitrary service** to elevate the privilege.

```
exeName_ = exeName + L".exe";
// ......
stream << L"\"" << Utils::getExePath() << L"\\" << exeName_ << "\" \"" << configFile << L"\"";
serviceCmdLine = stream.str();
// ......
svcCtrl.installService(serviceName_.c_str(), serviceCmdLine.c_str(),
            L"Windscribe Wireguard Tunnel", L"Manages the Windscribe WireGuard tunnel connection",
            SERVICE_WIN32_OWN_PROCESS, SERVICE_DEMAND_START, L"Nsi\0TcpIp\0", true);
```

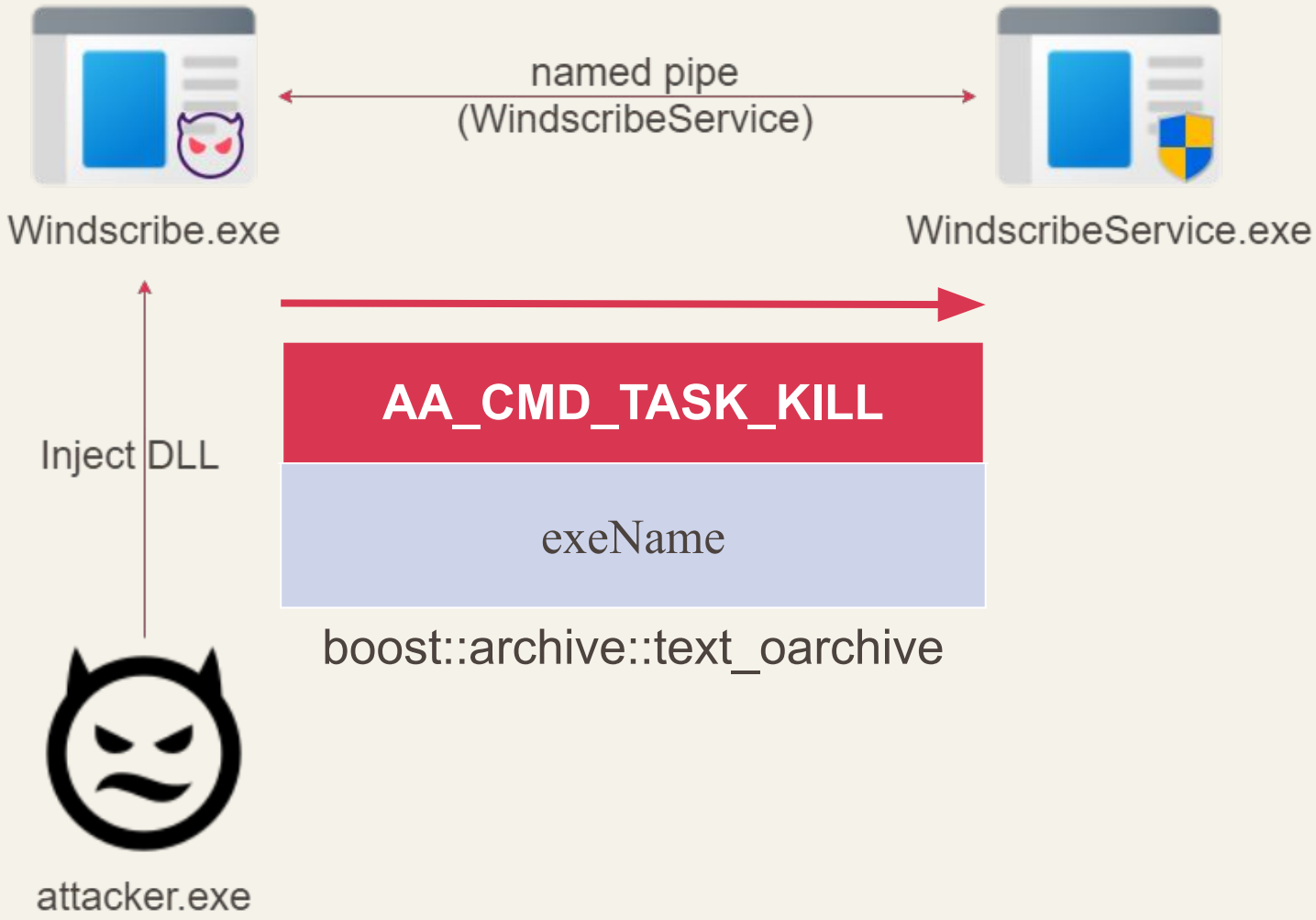
1. Controllable executable name.

Bypass the path with ..\..\..\attacker.exe

2. Install any service.

windscribe_service/wireguard/wireguardcontroller.cpp

Windscribe VuIn2



Windscribe VuIn2

TEAMT5 杜浦數位安全

AA_COMMAND_TASK_KILL: An authenticated user or guest can exploit the vulnerability to run arbitrary service to **kill any process** in the system.

Controllable executable name.

```
std::wstring killCmd = Utils::getSystemDir() + L"\\taskkill.exe /f /t /im " + cmdTaskKill.szExecutableName;
```

windscribe_service/process_command.cpp

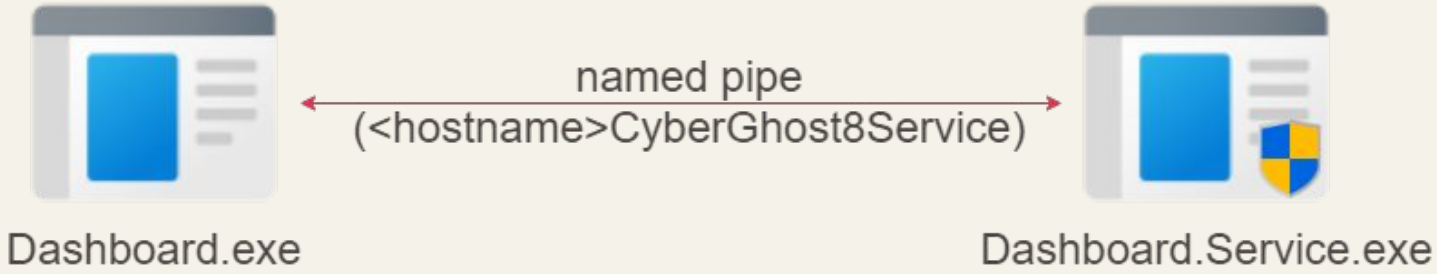
Windscribe Vuln1 Demo

PWN

PWN

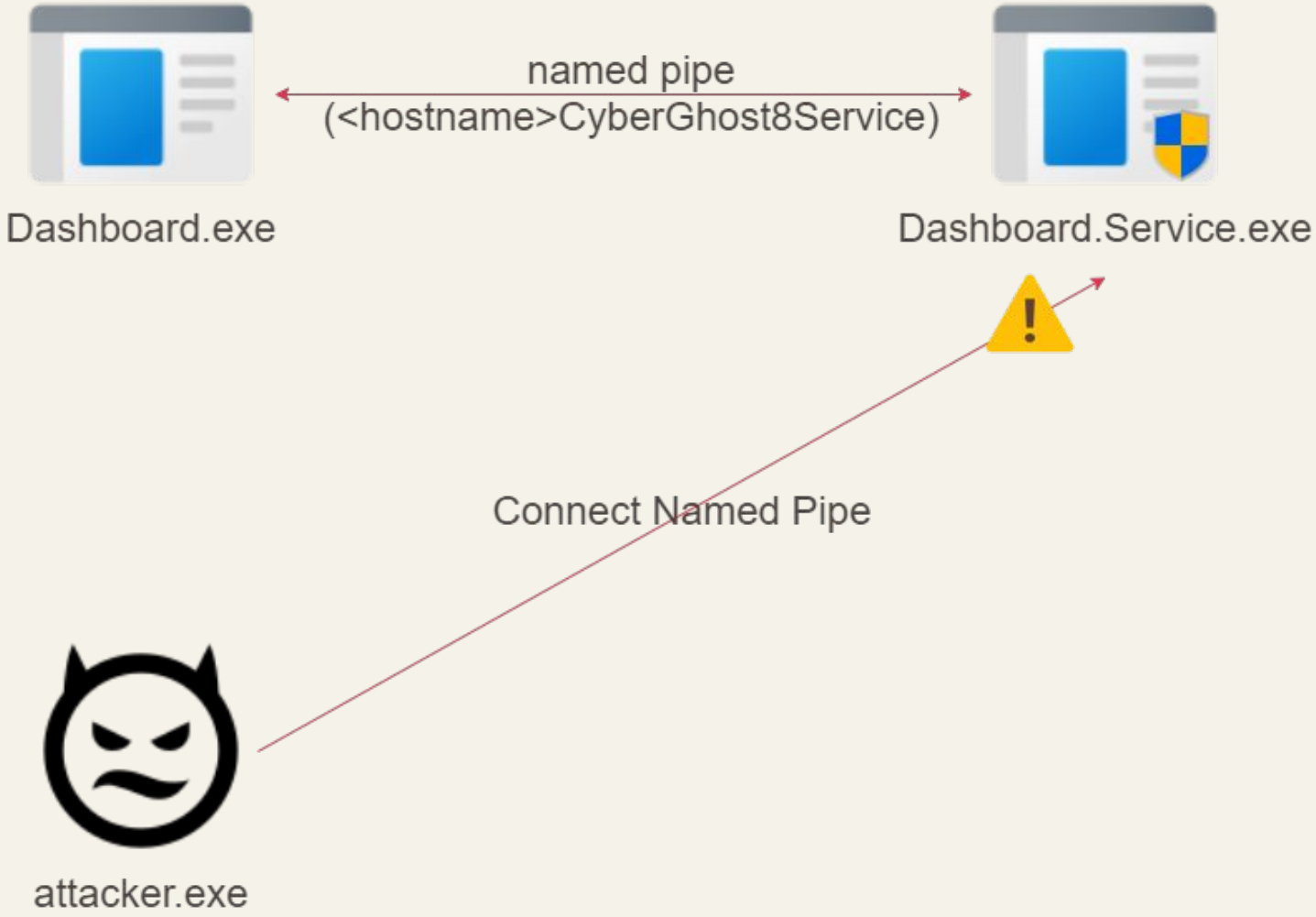
TEAMT5
杜 浦 數 位 安 全

CyberGhost Vulns

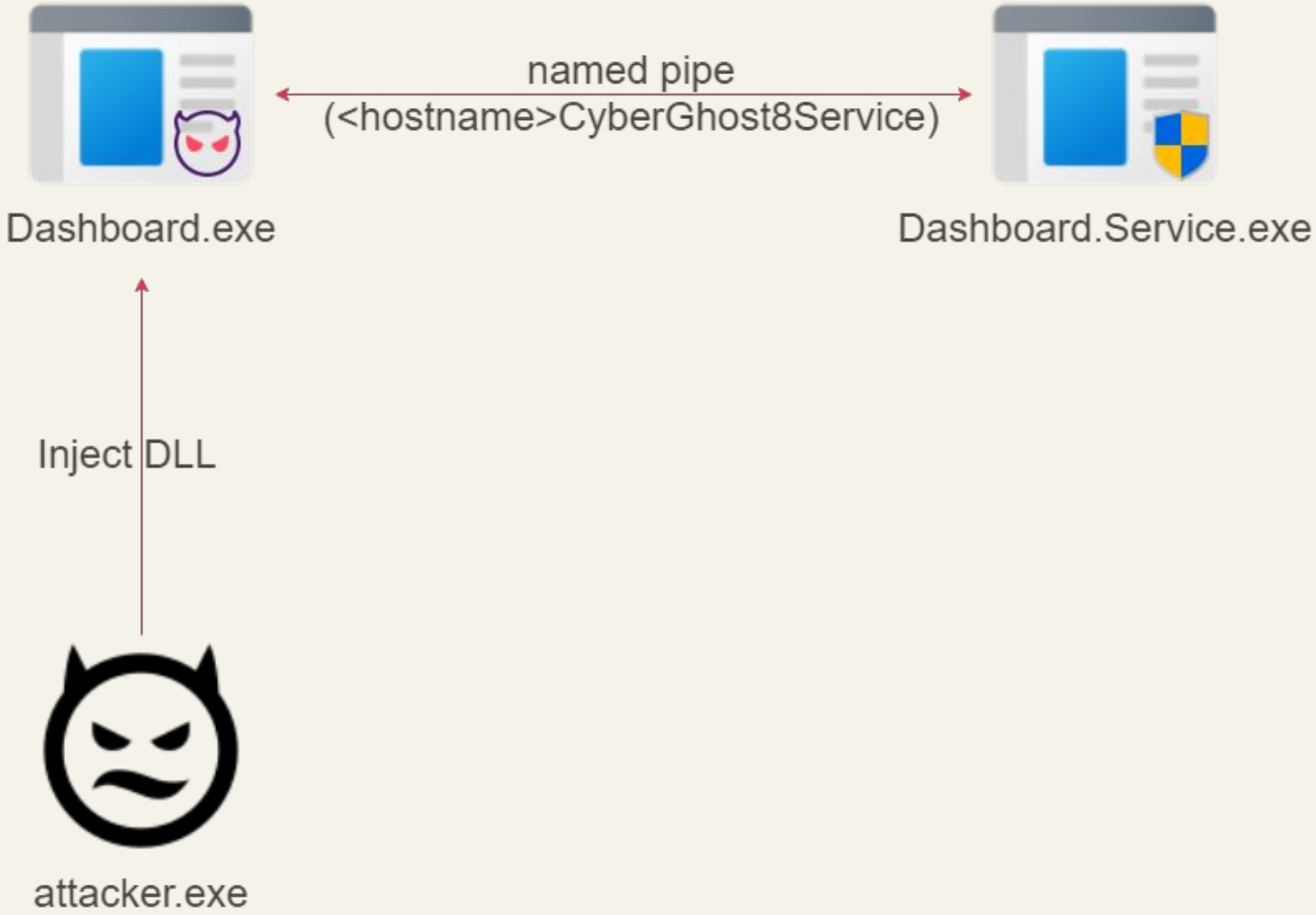



```
\\.\Pipe\<hostname>CyberGhost8Service
  RW NT AUTHORITY\Authenticated Users
  RW BUILTIN\Administrators
```

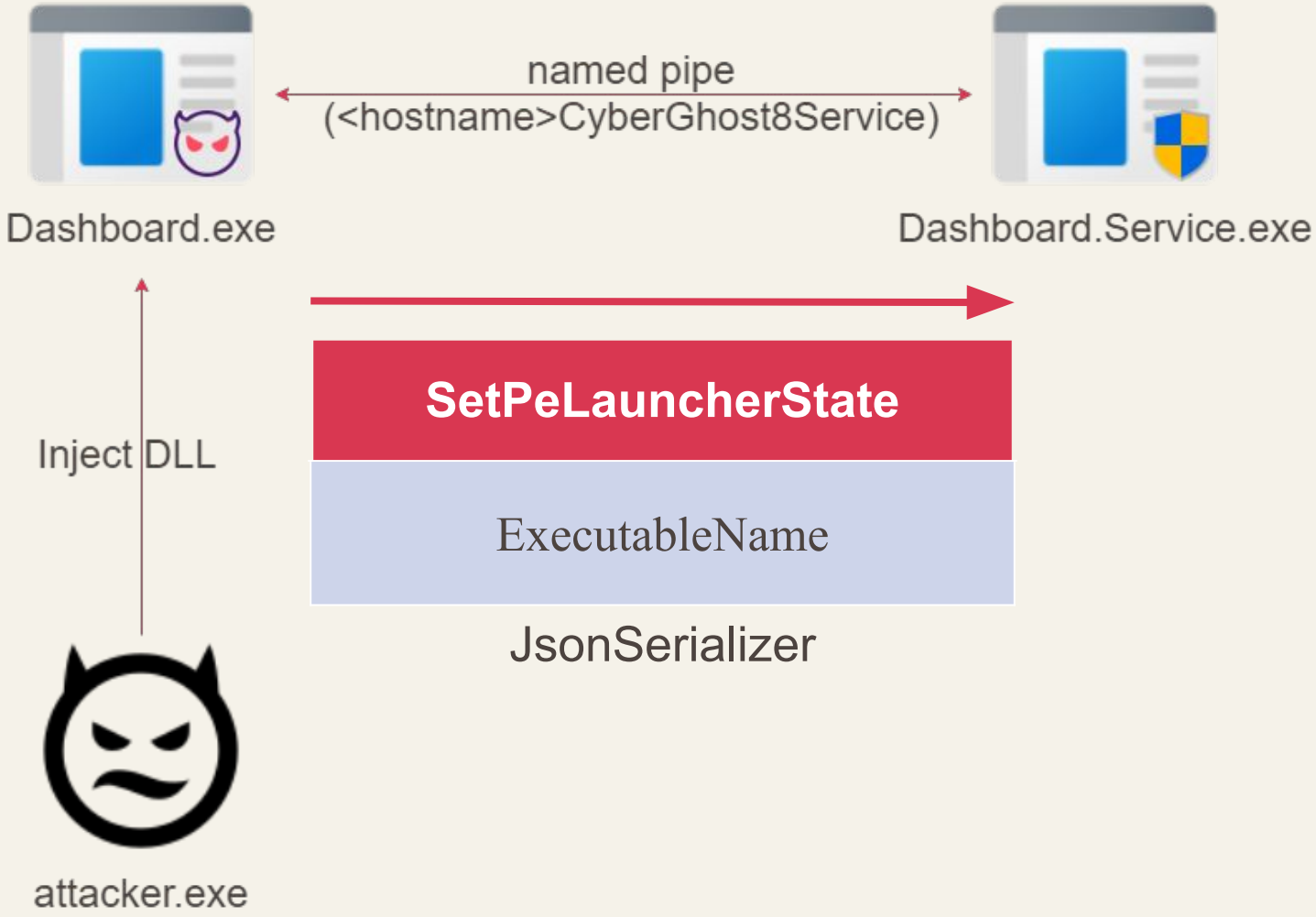
Image Check


named pipe
(<hostname>CyberGhost8Service)
Dashboard.exe
Dashboard.Service.exe
Connect Named Pipe
attacker.exe

Bypass Image Check



CyberGhost Vuln1



CyberGhost Vuln1

TEAMT5 杜浦數位安全

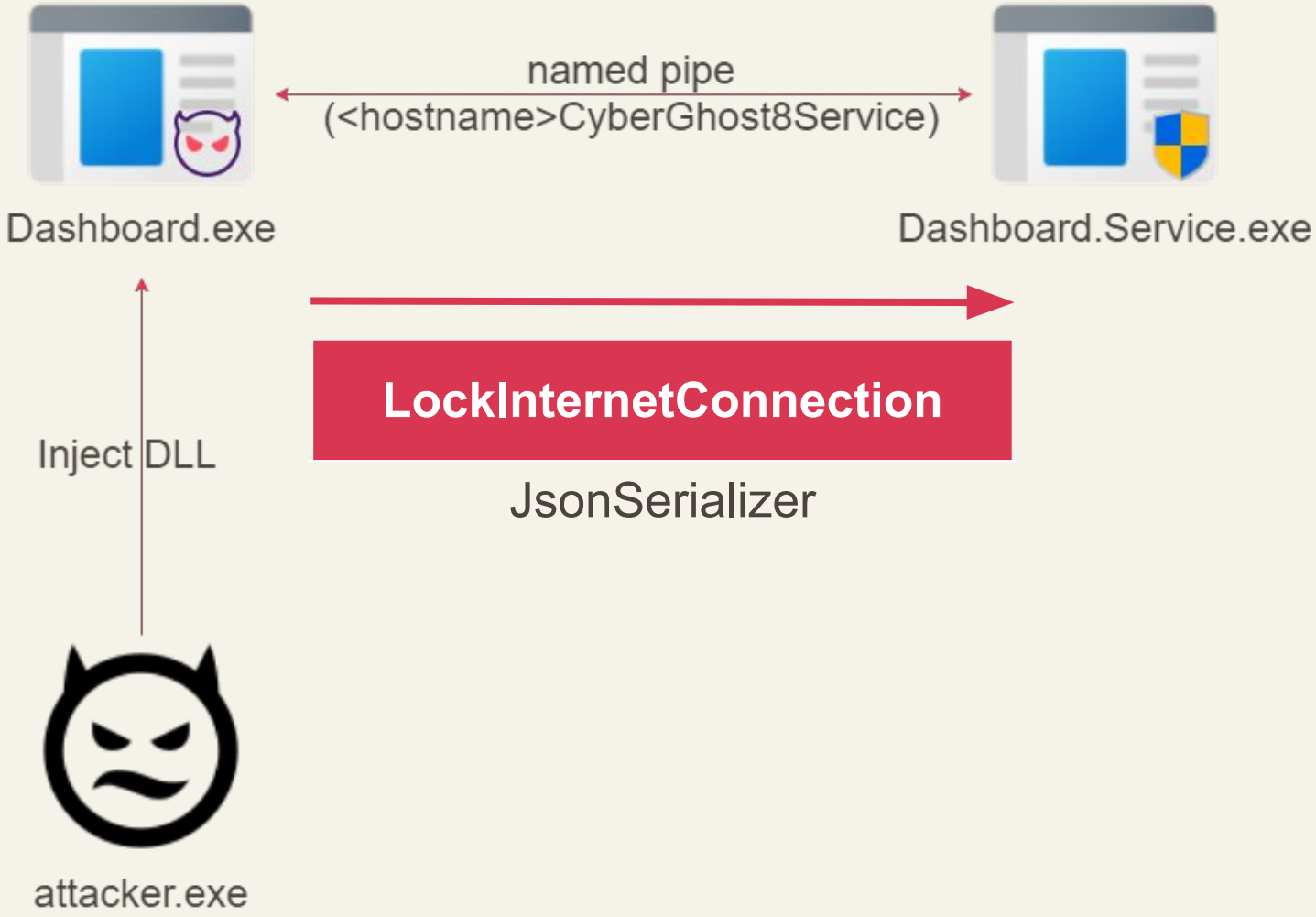
SetPeLauncherState: An authenticated user can exploit the vulnerability to **prevent any program from starting**.

```
using (RegistryKey registryKey2 =
    registryKey.OpenSubKey("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution
Options", RegistryKeyPermissionCheck.ReadWriteSubTree));
// ......
RegistryKey registryKey3 =
    registryKey2.CreateSubKey(peImageName, RegistryKeyPermissionCheck.ReadWriteSubTree);
// ......
registryKey3.SetValue("debugger", debuggerExecuteable);
// ......
```

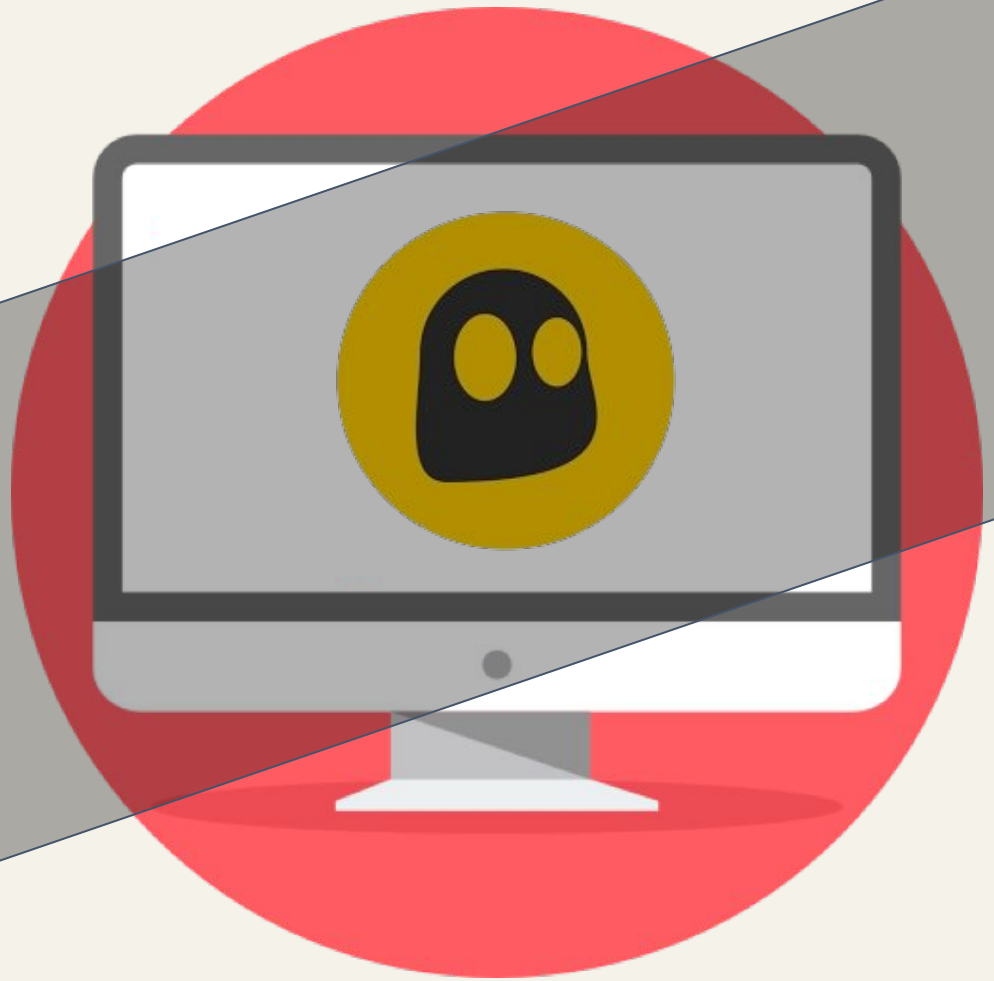
Controllable image name.

Set “debugger” value, but we can’t control the data.

CyberGhost VuIn2



CyberGhost Vuln1 Demo

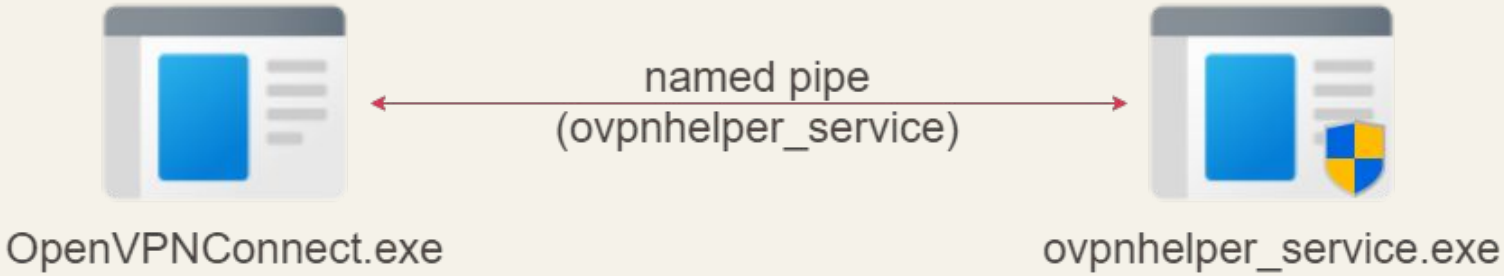


PWN

PWN

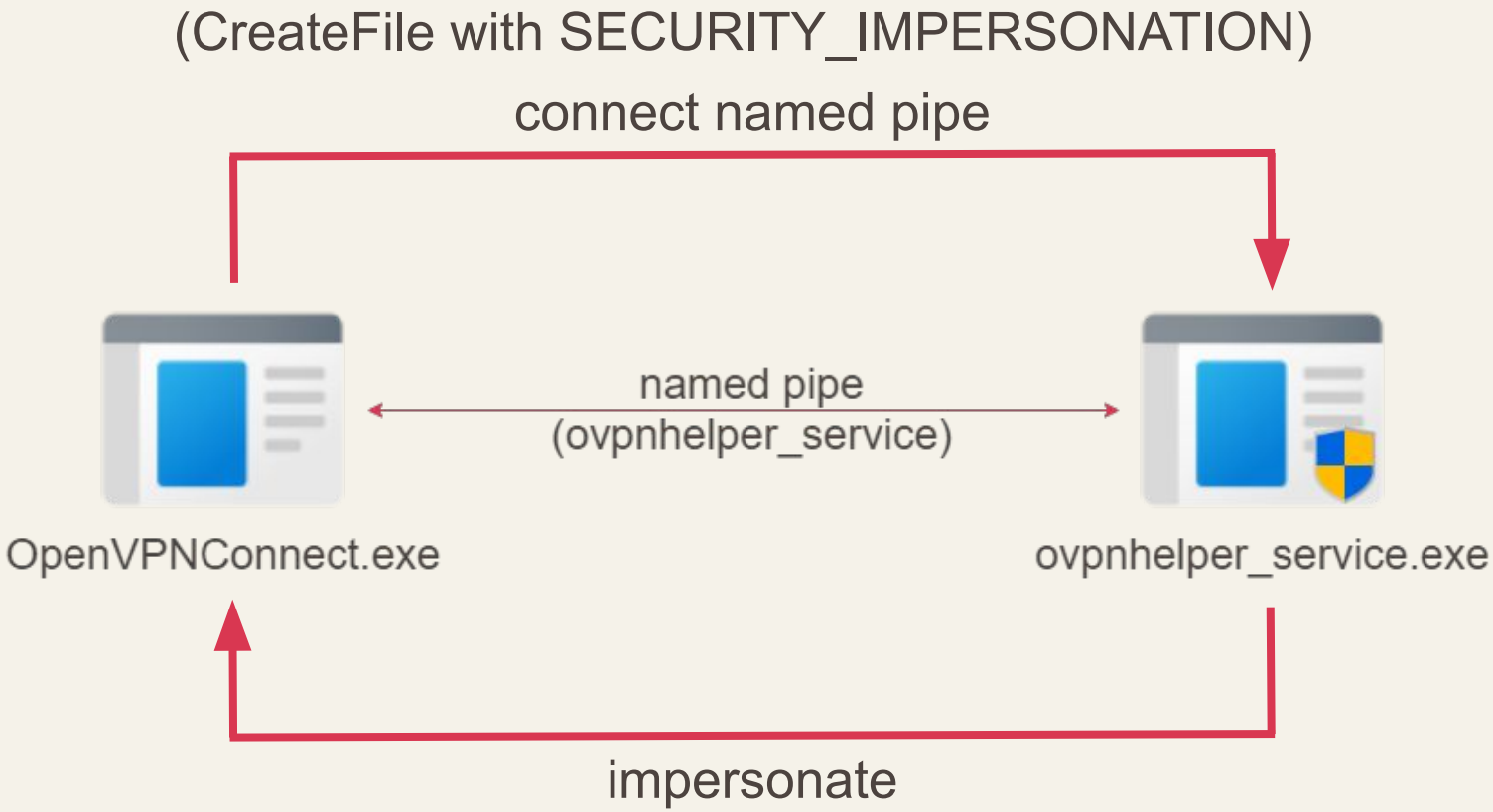
TEAMT5
杜 浦 數 位 安 全

OpenVPN VuIn

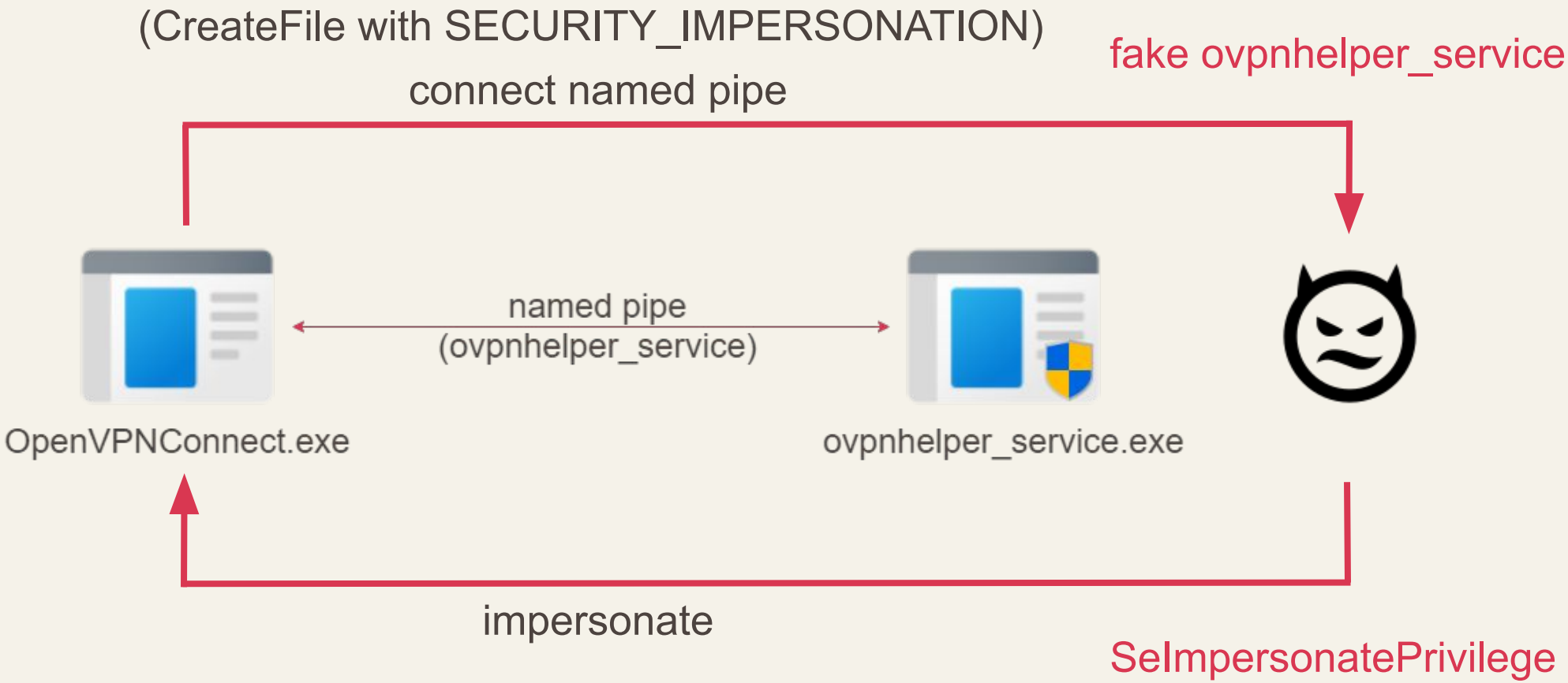



```
\\.\Pipe\ovpnhelper_service
  RW BUILTIN\Administrators
  RW NT AUTHORITY\SYSTEM
  RW NT AUTHORITY\Authenticated Users
  RW BUILTIN\Guests
```

OpenVPN VuIn



OpenVPN VuIn



OpenVPN Vuln Demo

PWN

PWN

TEAMT5
杜 浦 數 位 安 全

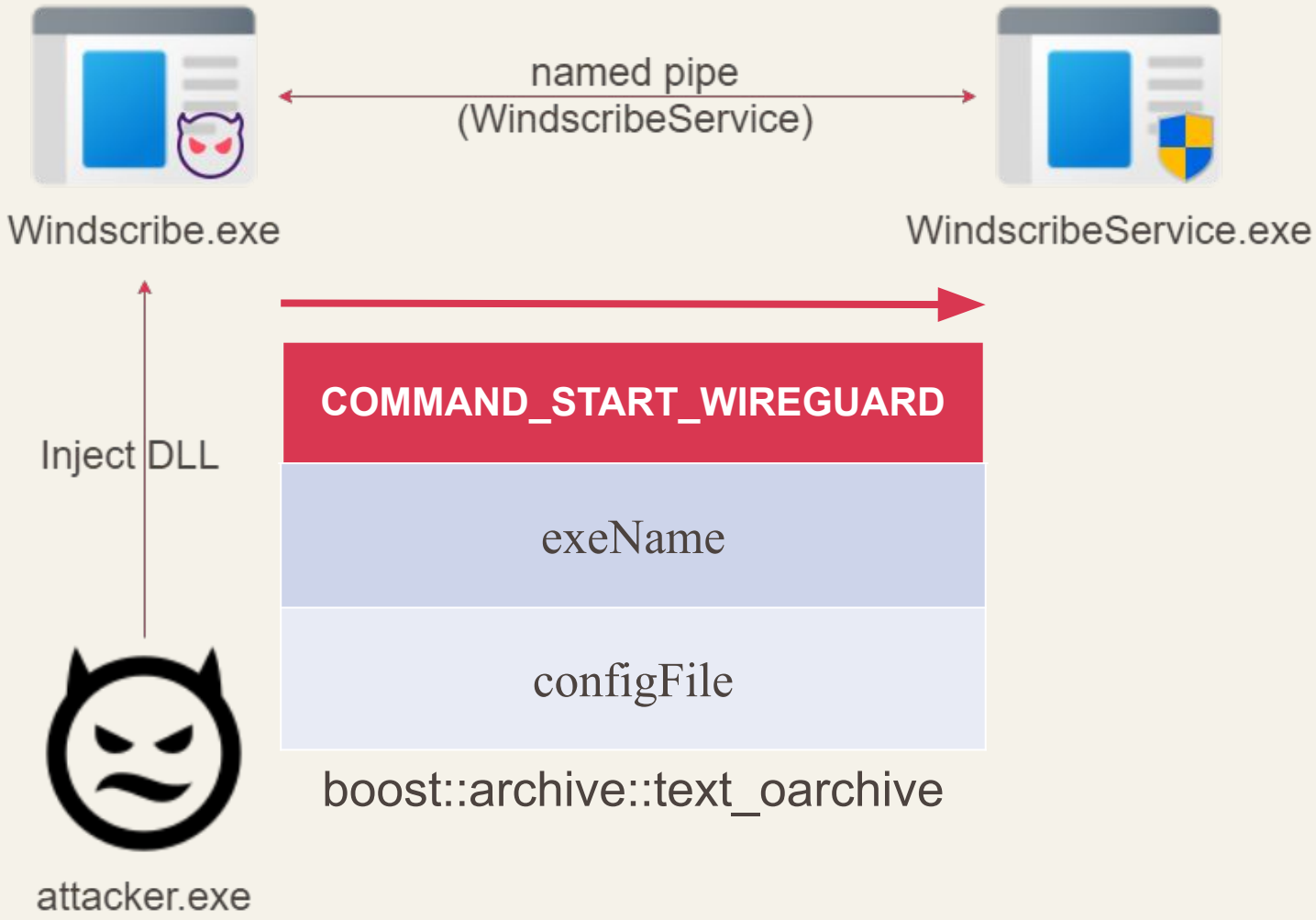
Fix

Fix for the vulnerabilities

Windscribe Vuln1 Fix

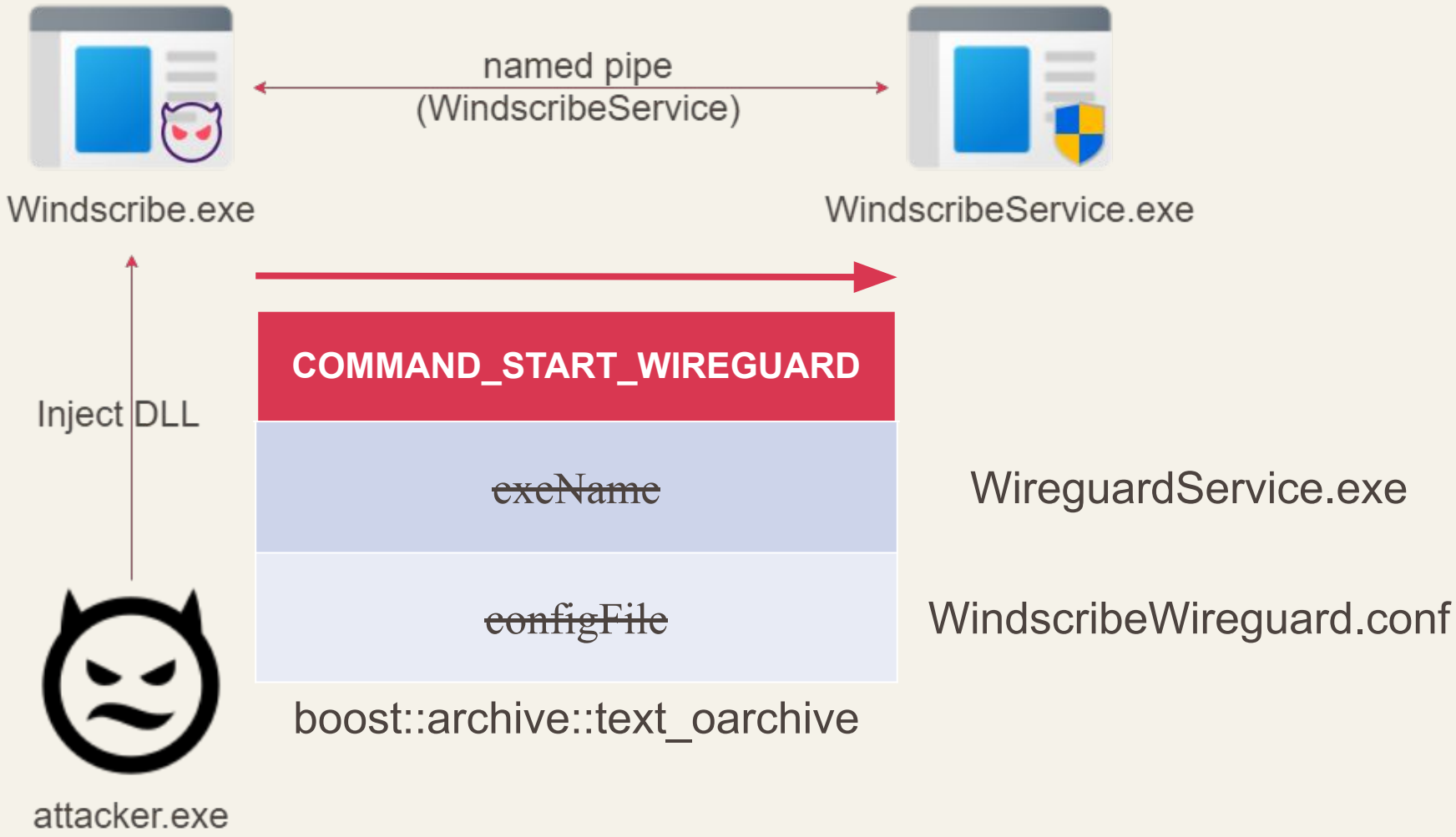
TEAMT5 杜浦數位安全

Original:



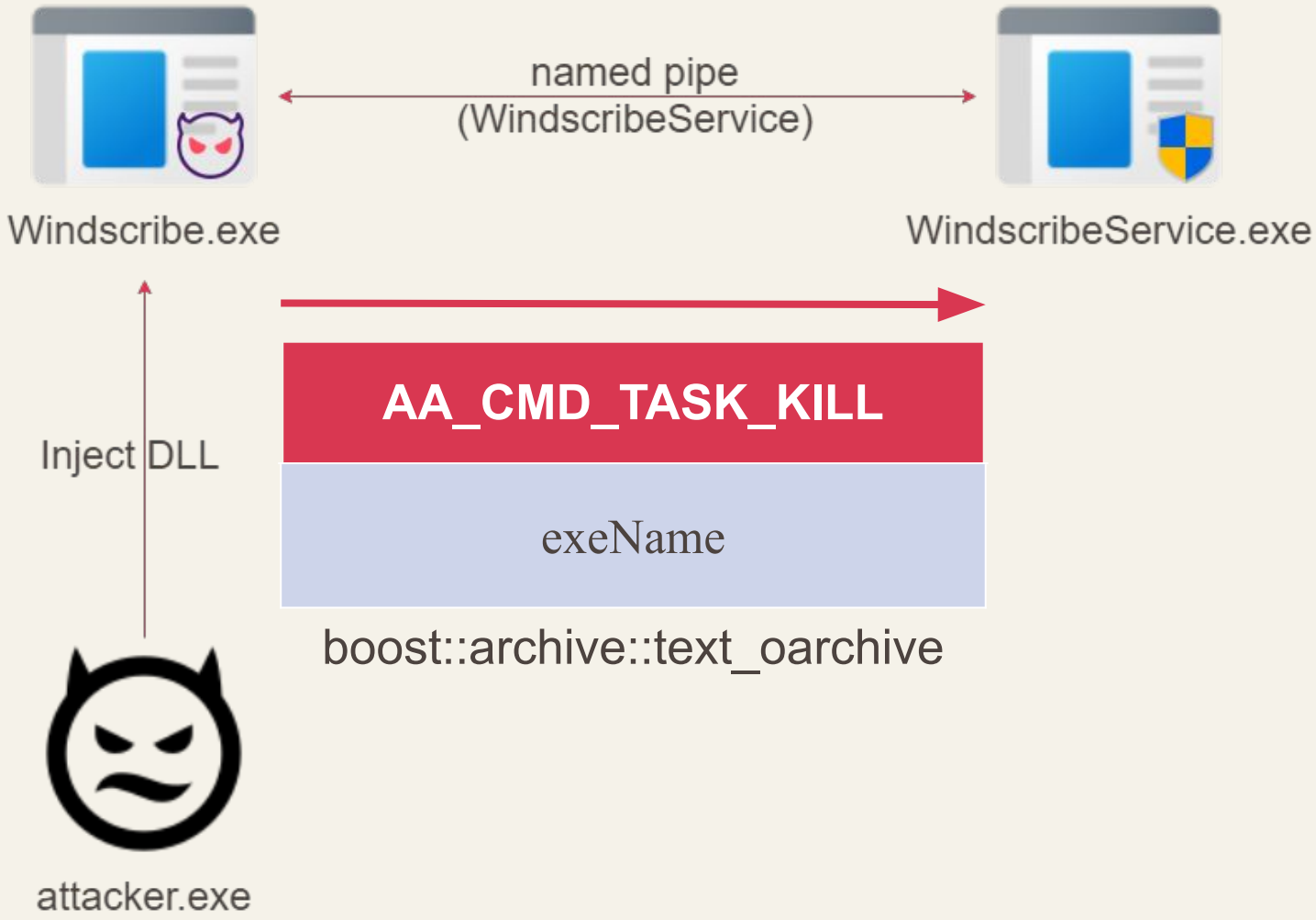
Windscribe Vuln1 Fix

Fixed:



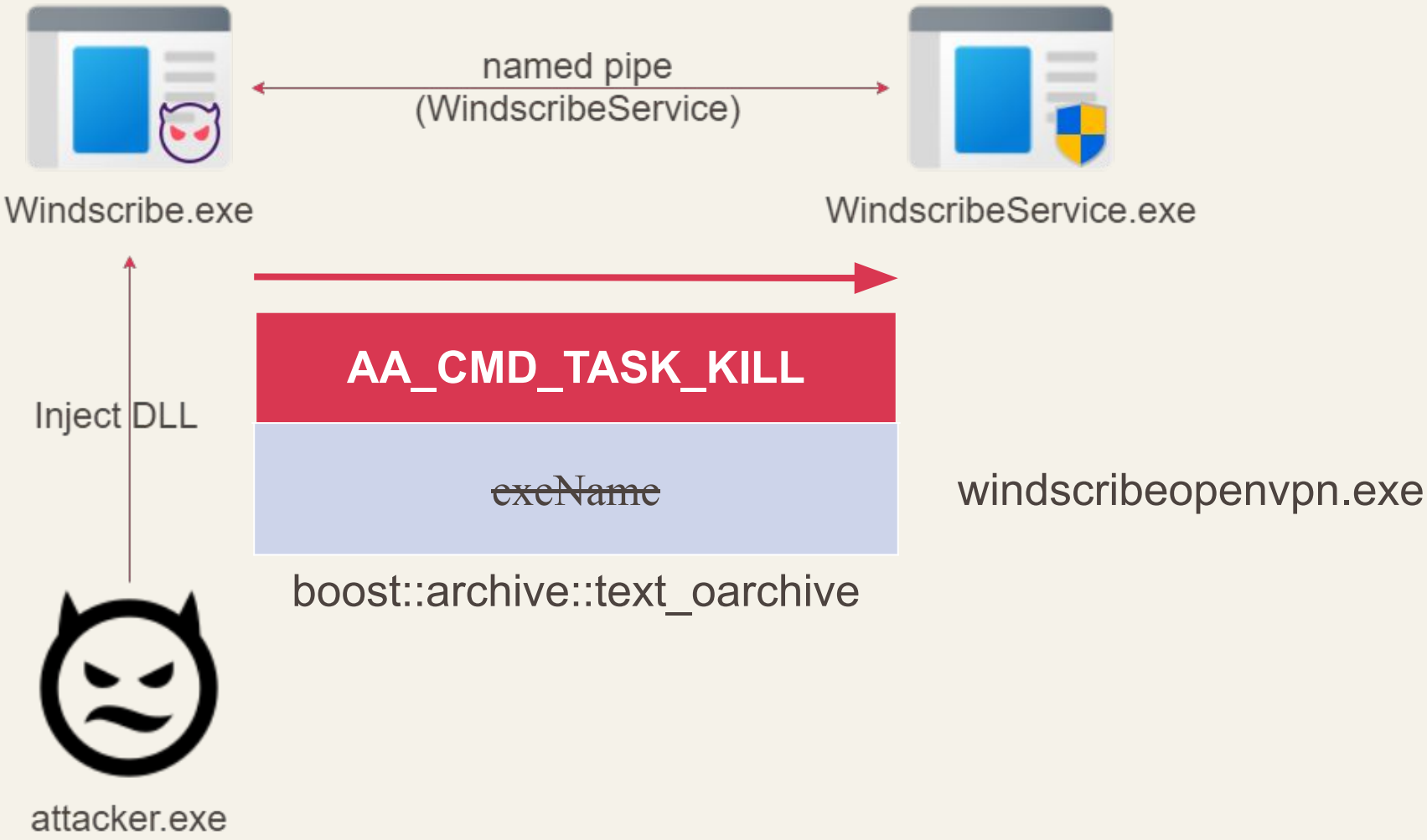
Windscribe Vuln2 Fix

Original:



Windscribe Vuln2 Fix

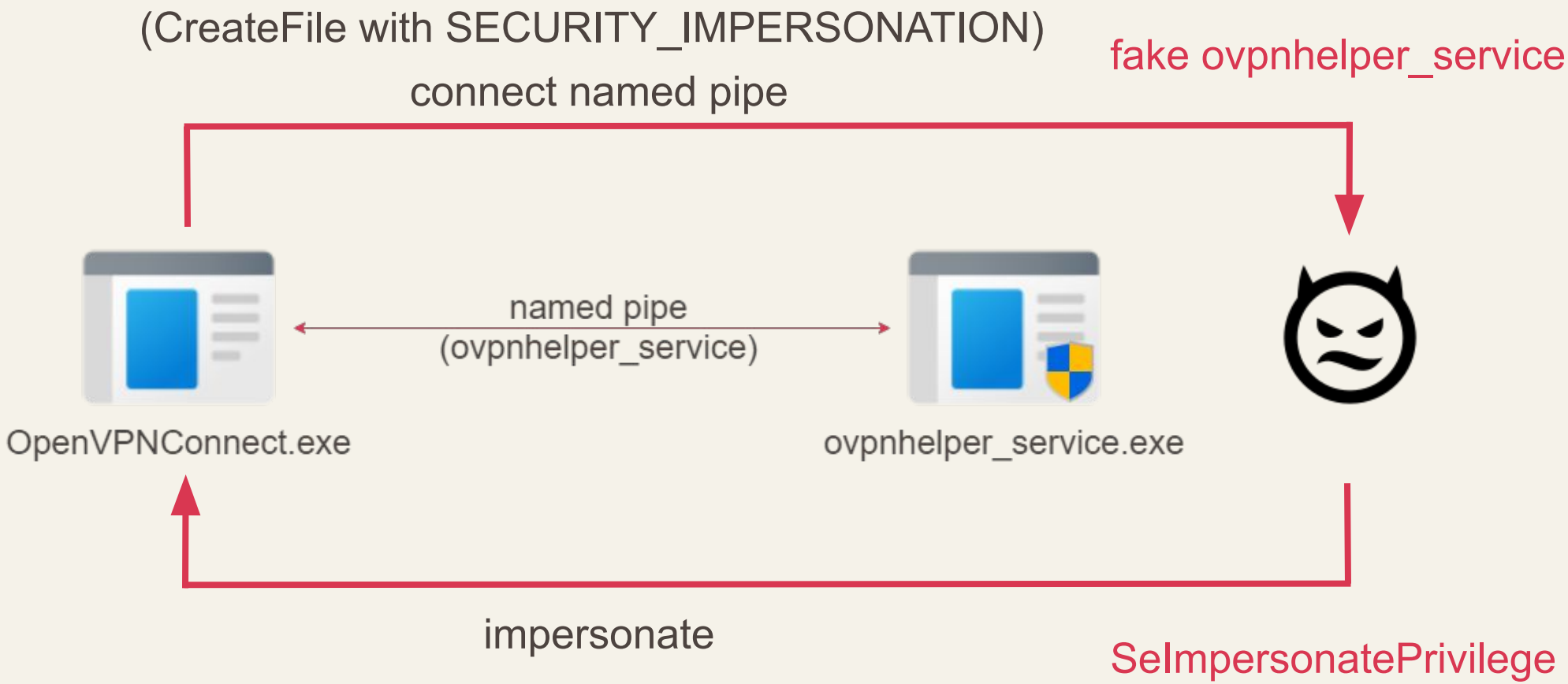
Fixed:



OpenVPN Vuln Fix

TEAMT5 杜浦數位安全

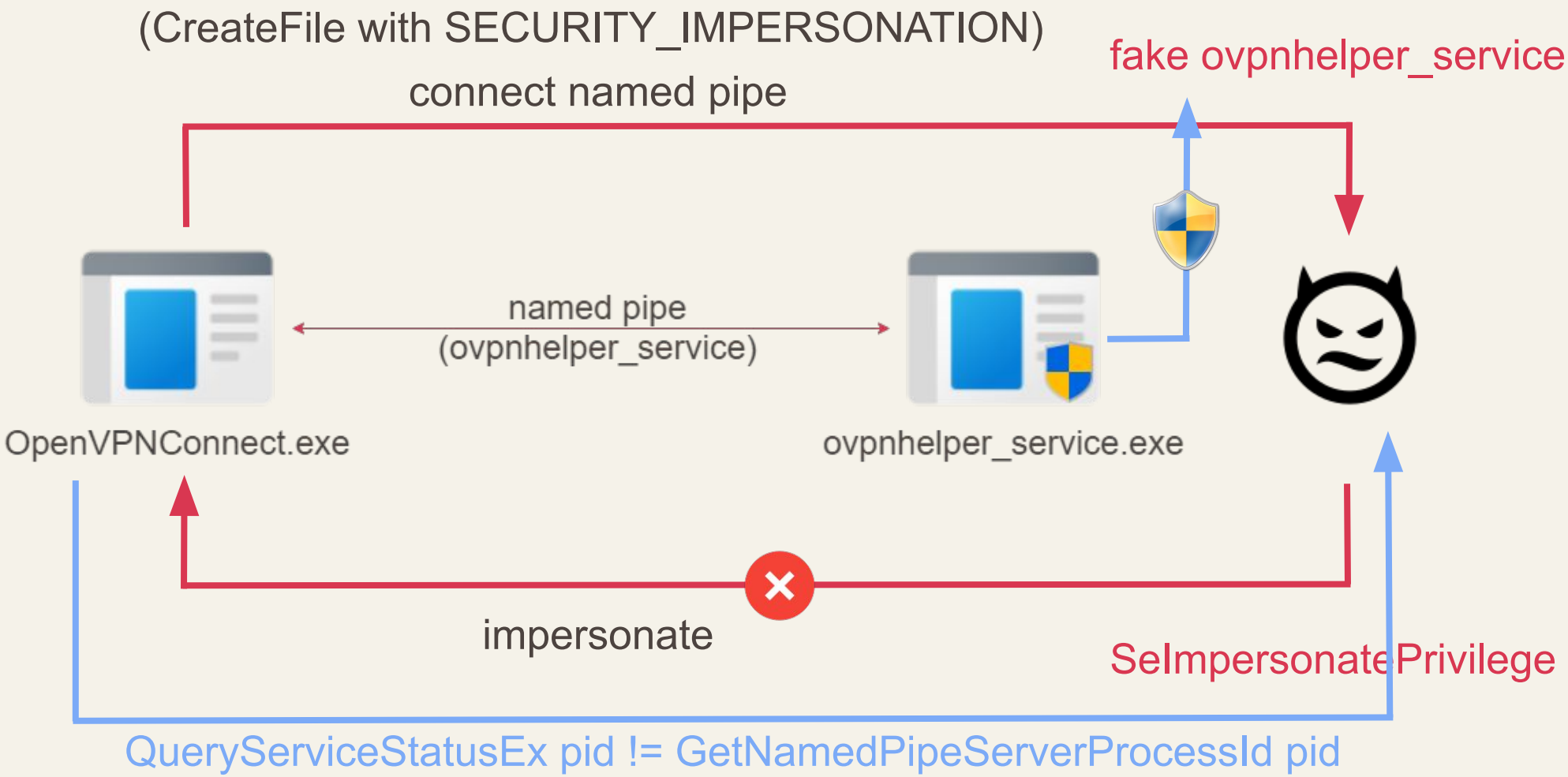
Original:



OpenVPN VuIn Fix

TEAMT5 杜浦數位安全

Fixed:



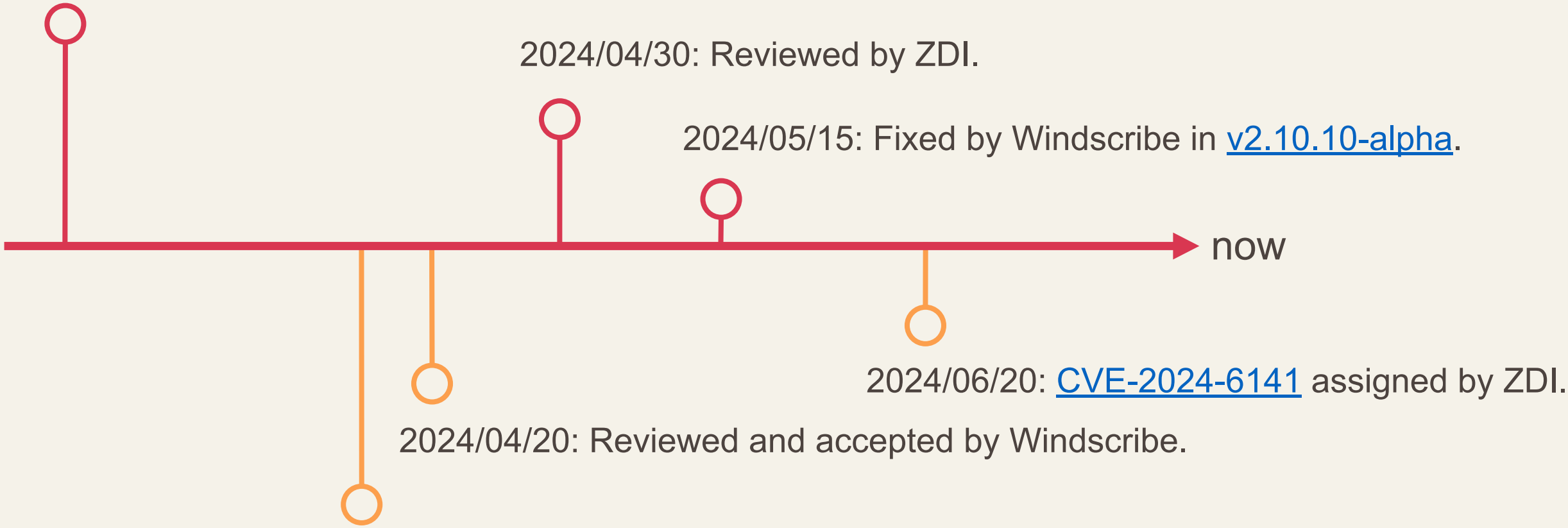
Report

Report submitted to each vendor and the timeline

Report Windscribe

TEAMT5 杜浦數位安全

2024/02/12: Report the EoP vulnerability (AA_COMMAND_START_WIREGUARD) to ZDI.



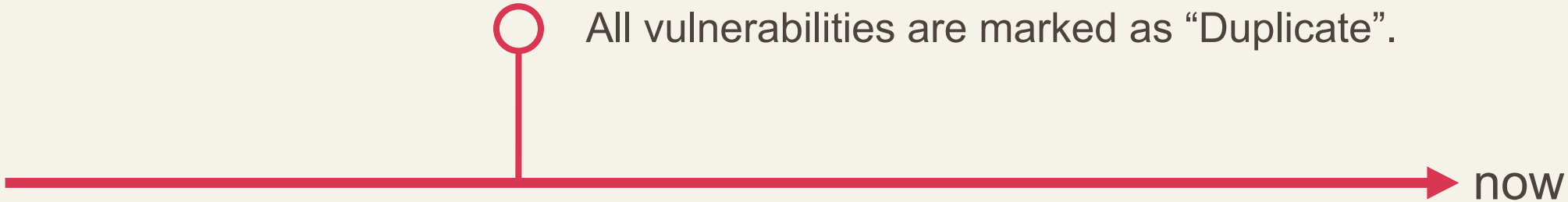
2024/04/19: Report the BAC vulnerabilities (AA_COMMAND_TASK_KILL) to Windscribe.

Report CyberGhost

TEAMT5
杜 浦 數 位 安 全

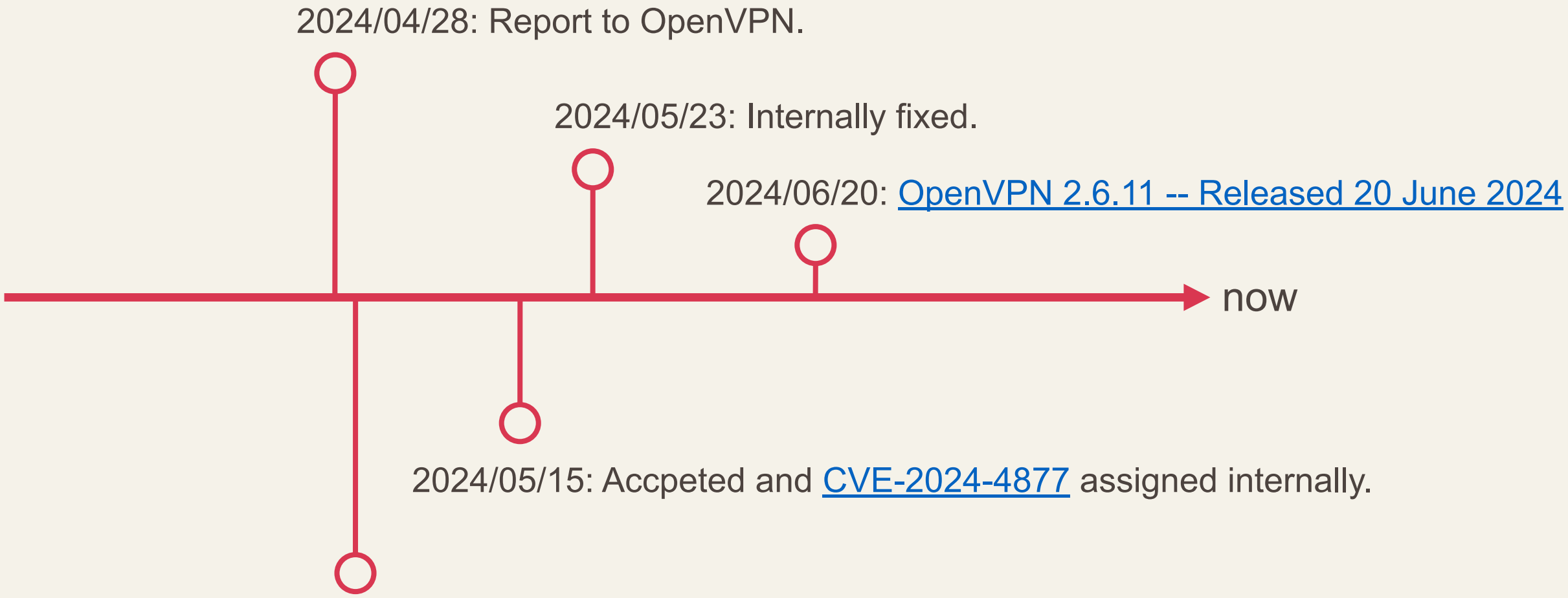
2024/04/19: Report to CyberGhost bounty program via Bugcrowd.

All vulnerabilities are marked as “Duplicate”.



Report OpenVPN

TEAMT5 杜浦數位安全



Takeaways

TEAMT5
杜 浦 數 位 安 全

- Named pipe is commonly used for IPC mechanism and impersonation.
- We can analyze named pipe operations more effectively with Ring3 Hook DLL and a minifilter driver.
- Vulnerabilities were found in 3 VPNs related to named pipe and how we can implement more securely.

Acknowledgement

TEAMT5 杜浦數位安全

Windscribe

CyberGhost

OpenVPN

Angelboy

L4ys

Kenny

Thanks For Listening!

zeze@teamt5.org

TEAMT5

杜 浦 數 位 安 全

Persistent Cyber Threat Hunters