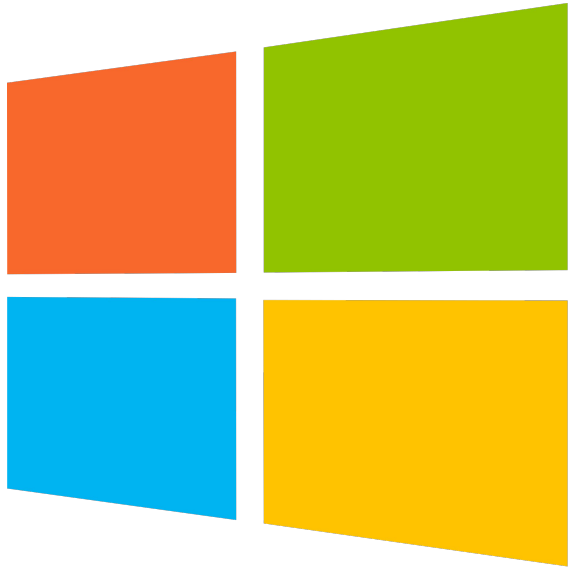
Windows Research Kernel

Niklas Schilli

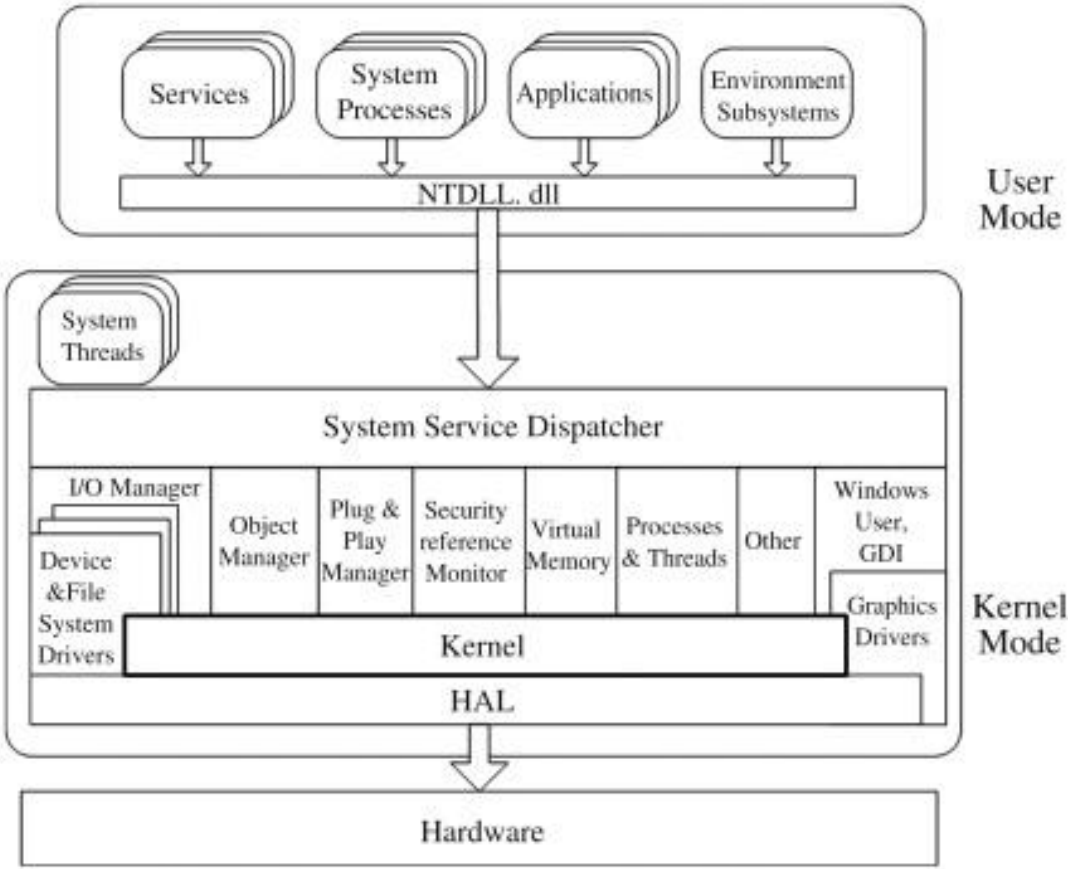


Überblick

- Aufbau des WRK
- Prozess: Toolgestützte analyse
- CVE Mapping

Recap: WRK

- Windows Kernel auf dem Stand von XP SP2/Windows Server 2003
- Größtenteils C Code
- Prebuilt Binaries für viele Komponenten wie z.B. HAL
- Über 800k LOC
- Einige fehlende Komponenten wie Power Management, Driver Verifier, Branding
- Beinhaltet Design Documents / Source Reference


Services
System Processes
Applications
Environment Subsystems
NTDLL. dll
User Mode
System Threads
System Service Dispatcher
I/O Manager
Device &File System Drivers
Object Manager
Plug & Play Manager
Security reference Monitor
Virtual Memory
Processes & Threads
Other
Windows User, GDI
Graphics Drivers
Kernel
HAL
Kernel Mode
Hardware

Static Analyzer

- Erlauben einfach Klassen an Bugs zu finden
- Zusätzlich zu Compilerflags wie -wall, -wextra -pedantic,ubsan/asan
- CppCheck, PVS-Studio, Clang, Sonarqube
- Use after free, double free, malloc leak, freeing non heap allocated objects
- Microsoft benutzte Prefast, intern entwickeltes Tool
- Jetzt Teil von MSVC mit /analyze

Hürden

- Großteil der Exploits targeted code der vorkompiliert ist und nicht im WRK liegt
- Logikfehler oder fehlende Validierung an unterschiedlichen stellen wird nicht erkannt (Check von Privilegien o.Ä.)
- Analyzer hat Probleme mit C->ASM Übergängen
- Custom Free Funktionen verhindern analyse von use after free/double free etc.

Viva64-PVS Studio

- Static Code Analyzer for C,C++,C# und Java
- Build Integration via Visual Studio
- Microsoft ist Kunde, analysiert wurden
  - Visual C++ Runtime
  - Windows 8 Treiber
  - Roslyn, MSBuild u.v.m.

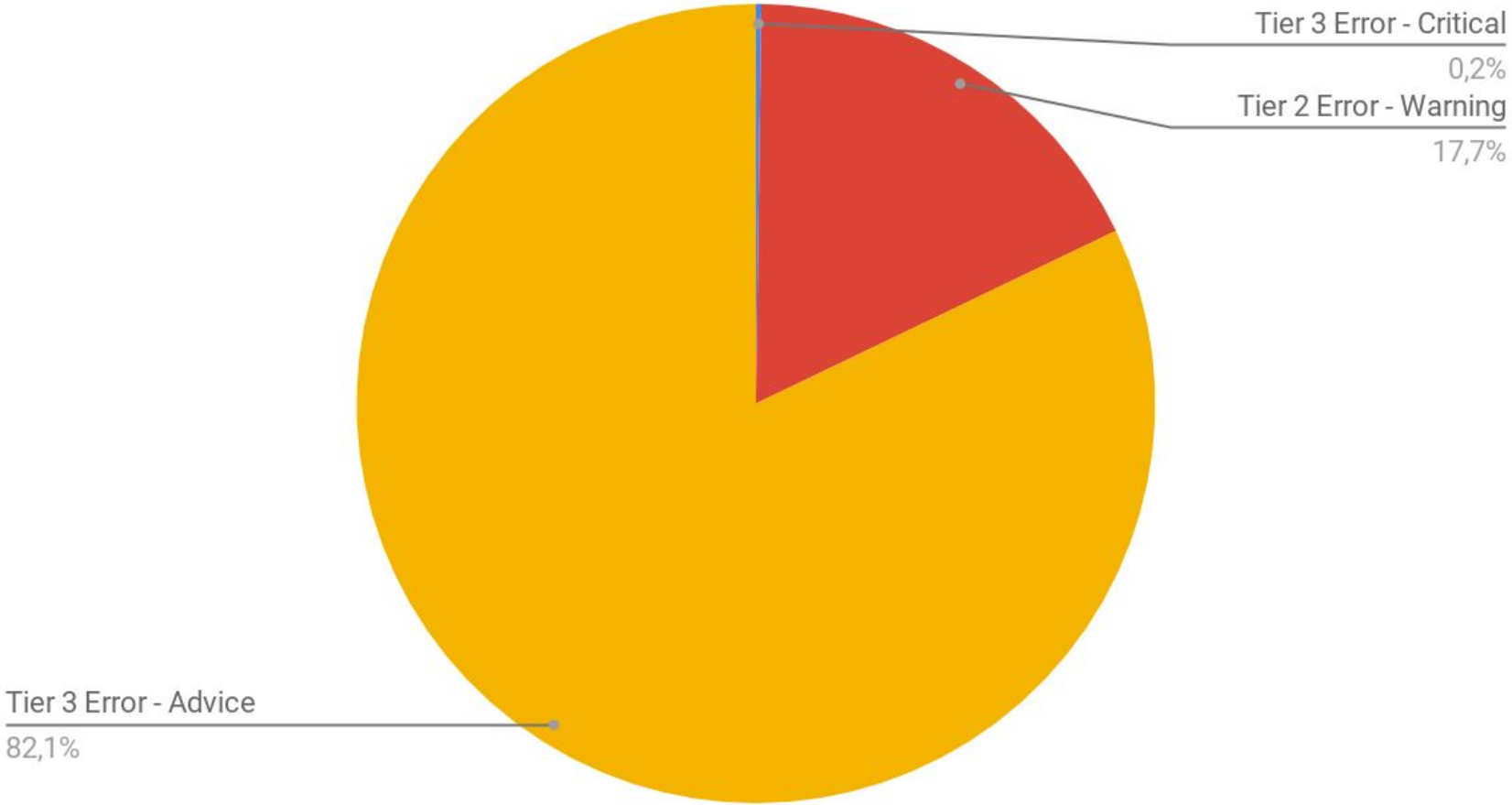
```
HRESULT get_accHelp(VARIANT varChild, BSTR *pszHelp)
{
  if ((varChild.vt == VT_I4) && (varChild.lVal == CHILDID_SELF))
  {
    *pszHelp = SysAllocString(L"ControlPane");
    return S_OK;
  }

  if (((varChild.vt != VT_I4) && (varChild.lVal != CHILDID_SELF))
      || (NULL == pszHelp))
  {
    return E_INVALIDARG;
  }
  ....
}
```

E_INVALIDARG sollte returned werden, stattdessen NPR

```
VARIANT foo;
foo.vt = VT_I4;
foo.lVal = CHILDID_SELF;
get_accHelp(foo, NULL);
```

PVS Studio Results



PVS-Studio Ergebnisse

- Tier 1 warnings sind größtenteils identisch mit pedantischen Compilerwarnings
- Comparison unsigned mit signed Werten, if then Conditions sollen gruppiert werden etc.
- Tier 2&3 warnings sind annotiert, meistens fehlende Validierung

```
Routine Description:

    Probe the incoming WNODE_ALL_DATA to ensure that any offsets in the
    header point to memory that is valid within the buffer. Also validate
    that the WNODE_ALL_DATA is properly formed.

    This routine MUST succeed before any fields in the WNODE_ALL_DATA can be
    used by any  kernel components when passed in from user mode. Note that
    we can trust that the input and output buffer are properly sized since
    the WMI IOCTLs are METHOD_BUFFERED and the IO manager does that for us.


    WNODE_ALL_DATA_RULES:

    1. Wnode is aligned on a 8 byte boundary
    2. The incoming buffer must be at least as large as sizeof(WNODE_HEADER)
    3. The outgoing buffer must be at least as large as sizeof(WNODE_ALL_DATA)
    5. WnodeHeader->BufferSize must equal incoming buffer size
```

Mapping CVE->WRK

- Meisten CVE’s nicht im WRK source
- Komponentenübergreifendes zusammenspiel von Fehlern
- Top 50 CVE’s für Windows XP sind nicht im WRK zu finden
- Fuzzing ist wahrscheinlich die bessere Alternative

1 CVE-2002-1257	Exec Code	2002-12-23	2019-04-30	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

Microsoft Virtual Machine (VM) up to and including build 5.0.3805 allows remote attackers to execute arbitrary code by including a Java applet that invokes COM (Component Object Model) objects in a web site or an HTML mail.

2 CVE-2003-0528	Exec Code Overflow	2003-09-17	2019-04-30	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

Heap-based buffer overflow in the Distributed Component Object Model (DCOM) interface in the RPCSS Service allows remote attackers to execute arbitrary code via a malformed RPC request with a long filename parameter, a different vulnerability than CVE-2003-0352 (Blaster/Nachi) and CVE-2003-0715.

3 CVE-2003-0715	Exec Code Overflow	2003-09-17	2019-04-30	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

Heap-based buffer overflow in the Distributed Component Object Model (DCOM) interface in the RPCSS Service allows remote attackers to execute arbitrary code via a malformed DCERPC DCOM object activation request packet with modified length fields, a different vulnerability than CVE-2003-0352 (Blaster/Nachi) and CVE-2003-0528.

4 CVE-2004-0201	Exec Code Overflow	2004-08-06	2019-04-30	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

Heap-based buffer overflow in the HtmlHelp program (hh.exe) in HTML Help for Microsoft Windows 98, Me, NT 4.0, 2000, XP, and Server 2003 allows remote attackers to execute arbitrary commands via a .CHM file with a large length field, a different vulnerability than CVE-2003-1041.

5 CVE-2004-0209	Exec Code	2004-11-03	2018-10-12	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

Unknown vulnerability in the Graphics Rendering Engine processes of Microsoft Windows 2000, Windows XP, and Windows Server 2003 allows remote attackers to execute arbitrary code via (1) Windows Metafile (WMF) or (2) Enhanced Metafile (EMF) image formats that involve "an unchecked buffer."

6 CVE-2004-0212	Exec Code Overflow	2004-08-06	2019-04-30	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

Stack-based buffer overflow in the Task Scheduler for Windows 2000 and XP, and Internet Explorer 6 on Windows NT 4.0, allows local or remote attackers to execute arbitrary code via a .job file containing long parameters, as demonstrated using Internet Explorer and accessing a .job file on an anonymous share.

7 CVE-2004-0214	DoS Exec Code Overflow	2004-11-03	2018-10-12	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

Buffer overflow in Microsoft Internet Explorer and Explorer on Windows XP SP1, WIndows 2000, Windows 98, and Windows Me may allow remote malicious servers to cause a denial of service (application crash) and possibly execute arbitrary code via long share names, as demonstrated using Samba.

8 CVE-2004-0568	Exec Code Overflow	2005-01-10	2019-04-30	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

HyperTerminal application for Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003 does not properly validate the length of a value that is saved in a session file, which allows remote attackers to execute arbitrary code via a malicious HyperTerminal session file (.ht), web site, or Telnet URL contained in an e-mail message, triggering a buffer overflow.

9 CVE-2004-0571	Exec Code	2005-01-10	2019-04-30	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

Microsoft Word for Windows 6.0 Converter does not properly validate certain data lengths, which allows remote attackers to execute arbitrary code via a .wri, .rtf, and .doc file sent by email or malicious web site, aka "Table Conversion Vulnerability," a different vulnerability than CVE-2004-0901.

10 CVE-2004-0575	Exec Code Overflow	2004-11-03	2018-10-12	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

Integer overflow in DUNZIP32.DLL for Microsoft Windows XP, Windows XP 64-bit Edition, Windows Server 2003, and Windows Server 2003 64-bit Edition allows remote attackers to execute arbitrary code via compressed (zipped) folders that involve an "unchecked buffer" and improper length validation.

11 CVE-2004-0840	Exec Code	2004-11-03	2018-10-12	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

The SMTP (Simple Mail Transfer Protocol) component of Microsoft Windows XP 64-bit Edition, Windows Server 2003, Windows Server 2003 64-bit Edition, and the Exchange Routing Engine component of Exchange Server 2003, allows remote attackers to execute arbitrary code via a malicious DNS response message containing length values that are not properly validated.

12 CVE-2004-0897	Exec Code Overflow	2005-01-11	2018-10-12	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

The Indexing Service for Microsoft Windows XP and Server 2003 does not properly validate the length of a message, which allows remote attackers to execute arbitrary code via a buffer overflow attack.

13 CVE-2004-0901	Exec Code	2005-01-10	2019-04-30	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

Microsoft Word for Windows 6.0 Converter (MSWRD632.WPC), as used in WordPad, does not properly validate certain data lengths, which allows remote attackers to execute arbitrary code via a .wri, .rtf, and .doc file sent by email or malicious web site, aka "Font Conversion Vulnerability," a different vulnerability than CVE-2004-0571.

14 CVE-2004-2289	Exec Code	2004-12-31	2018-10-12	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete

Microsoft Windows XP Explorer allows local users to execute arbitrary code via a system folder with a Desktop.ini file containing a .ShellClassInfo specifier with a CLSID value that is associated with an executable file.

Quellen

- https://ars.els-cdn.com/content/image/1-s2.0-S0895717709003409-gr2.jpg, Zugriff 11.05.2020 14:00
- https://www.viva64.com/en/a/0077/#ID0EJIBI, Zugriff 11.05.2020 15:00
- https://docs.microsoft.com/en-us/cpp/build/reference/analyze-code-analysis?view=vs-2019,Zugriff 12.05.2020 11:00
- https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-739/Microsoft-Windows-Xp.html, Zugriff 12.05.2020 12:00
- https://www.cvedetails.com/vulnerability-list.php?vendor_id=26&product_id=739&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&month=0&cweid=0&order=3&trc=741&sha=96656e0273b52e8473fbf8b6371fe2ed4a0f8ae8