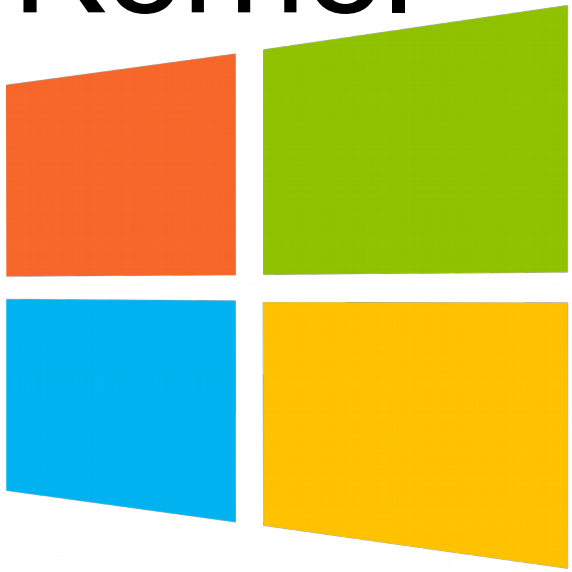
Windows Research Kernel

Niklas Schilli



Überblick

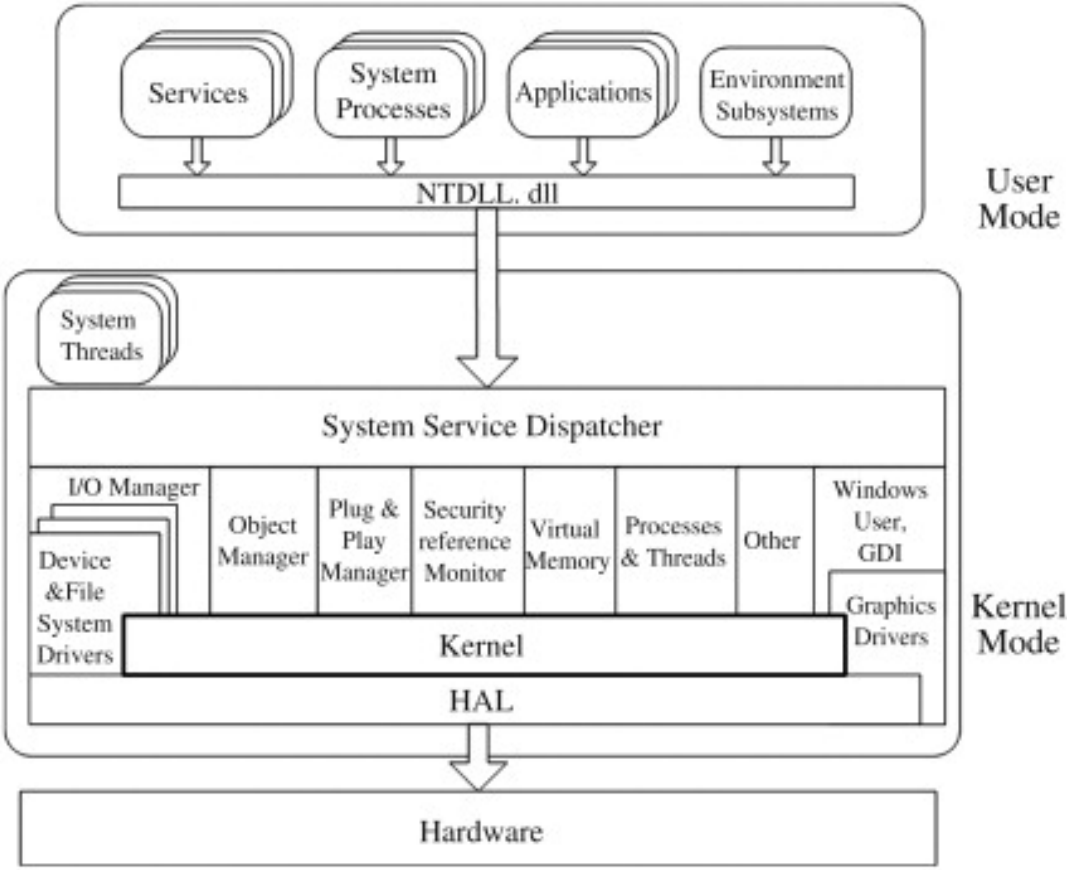
- Was ist der WRK?
- Aufbau
- Static Analyzers
- Durchführung des Projektes

Overview: WRK

- Ursprünglich von Microsoft an Universitäten lizensiert
- Windows Kernel auf dem Stand von XP SP2/Windows Server 2003
- Wahrscheinlich als Grundlage für ReactOS benutzt worden
- Forschungsgegenstand am HPI, z.B. Microsoft Phoenix Integration in den WRK / Microsoft Research Singularity / Midori
- Ausschließlich C / Assembler

Aufbau

- Enhält Kernelkomponenten wie Memory Manager, Scheduler, IO
- Hohes Maß an Nebenläufigkeit
- HAL, Bootvid u.A. sind vorgebaut
- Hinzufügen von Syscalls ist möglich



https://ars.els-cdn.com/content/image/1-s2.0-S0895717709003409-gr2.jpg

Static Analyzer

- Erlauben einfach Klassen an Bugs zu finden
- Zusätzlich zu -wall, -wextra -pedantic,ubsan/asan
- GCC 10 enthält static analyzer die angeschaltet werden können
- 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

```c
#include <stdlib.h>

void test(void *ptr)
{
    free(ptr);
    free(ptr);
}
```

```
$ gcc -c -fanalyzer double-free-1.c
double-free-1.c: In function ‘test’:
double-free-1.c:6:3: warning: double-‘free’ of ‘ptr’ [CWE-415] [-Wanalyzer-double-free]
    6 |   free(ptr);
      |   ^~~~~~~~~
  ‘test’: events 1-2
    |
    |    5 |   free(ptr);
    |      |   ^~~~~~~~~
    |      |   |
    |      |   (1) first ‘free’ here
    |    6 |   free(ptr);
    |      |   ~~~~~~~~~
    |      |   |
    |      |   (2) second ‘free’ here; first ‘free’ was at (1)
    |
```

```
static const PCHAR Nv11Board = "NV11 (GeForce2) Board";
static const PCHAR Nv11Chip = "Chip Rev B2";
static const PCHAR Nv11Vendor = "NVidia Corporation";

BOOLEAN
IsVesaBiosOk(...)
{
  ...
  if (!(strncmp(Vendor, Nv11Vendor, sizeof(Nv11Vendor))) &&
      !(strncmp(Product, Nv11Board, sizeof(Nv11Board))) &&
      !(strncmp(Revision, Nv11Chip, sizeof(Nv11Chip))) &&
      (OemRevision == 0x311))
  ...
}
```

Sizeof NV11… == sizeof(void*), da NV11 = const char *
https://www.viva64.com/en/a/0077/#ID0EJIBI

```
static void REGPROC_unescape_string(WCHAR* str)
{
  ...
  default:
    fprintf(stderr,
      "Warning! Unrecognized escape sequence: \\%c'\n",
      str[str_idx]);
  ...
}
```

%c -> %C da WChar

https://www.viva64.com/en/a/0077/#ID0EJIBI

Ziel des Projekts

- Besseres Verständnis von Windows Internas
- Abgleich Toolergebnisse, irgendwelche bugs/vulnerabilities?
- ReactOS hat per Analyzer auffindbare bugs, hat der WRK das selbe Problem?
- CVE Mapping auf den source code des WRK

Microsoft » Windows Xp : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **741** Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-0708	20		Exec Code	2019-05-16	2019-07-15	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.														
2	CVE-2017-8487			Exec Code	2017-06-15	2019-10-02	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Windows OLE in Windows XP and Windows Server 2003 allows an attacker to execute code when a victim opens a specially crafted file or program aka "Windows olecnv32.dll Remote Code Execution Vulnerability."														
3	CVE-2017-8461			Exec Code	2017-06-15	2019-10-02	6.9	None	Local	Medium	Not required	Complete	Complete	Complete
Windows RPC with Routing and Remote Access enabled in Windows XP and Windows Server 2003 allows an attacker to execute code on a targeted RPC server which has Routing and Remote Access enabled via a specially crafted application, aka "Windows RPC Remote Code Execution Vulnerability."														
4	CVE-2017-0176	120		Exec Code Overflow	2017-06-22	2019-10-02	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
A buffer overflow in Smart Card authentication code in gpkcsp.dll in Microsoft Windows XP through SP3 and Server 2003 through SP2 allows a remote attacker to execute arbitrary code on the target computer, provided that the computer is joined in a Windows domain and has Remote Desktop Protocol connectivity (or Terminal Services) enabled.														
5	CVE-2014-4971	20	3	+Priv	2014-07-26	2018-10-12	7.2	None	Local	Low	Not required	Complete	Complete	Complete
Microsoft Windows XP SP3 does not validate addresses in certain IRP handler routines, which allows local users to write data to arbitrary memory locations, and consequently gain privileges, via a crafted address in an IOCTL call, related to (1) the MQAC.sys driver in the MQ Access Control subsystem and (2) the BthPan.sys driver in the Bluetooth Personal Area Networking subsystem.														
6	CVE-2014-0323	200		DoS +Info	2014-03-12	2019-05-13	6.6	None	Local	Low	Not required	Complete	None	Complete
win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to obtain sensitive information from kernel memory or cause a denial of service (system hang) via a crafted application, aka "Win32k Information Disclosure Vulnerability."														
7	CVE-2014-0317	20		Bypass	2014-03-12	2019-05-08	5.4	None	Remote	High	Not required	None	Complete	None

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://gcc.gnu.org/onlinedocs/gcc/Static-Analyzer-Options.html, Zugriff 11.05.2020 16:00
- https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-739/Microsoft-Windows-Xp.html, Zugriff 12.05.2020 12:00