

🔗 master


🌿 1 branch

🏷 0 tags

Go to file

Add file

<> Code

 yeyintminthuhtut Merge pull request #3 from GorZ3rk/master 

...

787495b on Jan 13, 2022 22 commits

📄 LICENSE	Initial commit	4 years ago
📄 README.md	add new contents	3 years ago

☰ README.md

# Awesome Advanced Windows Exploitation References

List of Awesome Advanced Windows Exploitation References

This list is for anyone wishing to upgrade on their Windows Exploitation Knowledge.

Anyway, this is a living resources and will update regularly with latest research articles/talks of awesome researchers.

Kudos to all orignial authors of each research ref.

You can help by sending Pull Requests to add more information. or ping me @yeyint\_mth

## Table of Contents

- Browser
- Mitigation Bypass
- Kernel
- Misc

### ↑ Browser

- Beginners guide to UAT exploits IE 0day exploit development
- Fuzzy Security - Spraying the Heap [Chapter 1: Vanilla EIP] – Putting Needles in the Haystack
- Fuzzy Security - Spraying the Heap [Chapter 2: Use-After-Free] – Finding a needle in a Haystack
- Anatomy of an exploit – inside the CVE-2013-3893 Internet Explorer zero-day – Part 1
- Using the JIT Vulnerability to Pwn Microsoft Edge
- Post-mortem Analysis of a Use-After-Free Vulnerability (CVE-2011-1260)
- Advanced Heapspraying Technique
- HeapSpray Aurora Vulnerability
- Microsoft Edge Chakra JIT Type Confusion CVE-2019-0539
- CVE-2019-0539 Root Cause Analysis
- attacking javascript engines
- Learning browser exploitation via 33C3 CTF feuerfuchs challenge
- A Methodical Approach to Browser Exploitation
- Reducing target scope within JSC, building a JavaScript fuzzer
- Performing root-cause analysis of a JSC vulnerability
- Weaponizing a JSC vulnerability for single-click RCE
- Evaluating the Safari sandbox, and fuzzing WindowServer on MacOS
- Weaponizing a Safari sandbox escape
- Microsoft Edge MemGC Internals
- The ECMA and the Chakra
- Memory Corruption Exploitation In Internet Explorer
- IE 0day Analysis And Exploit
- Write Once, Pwn Anywhere
- The Art of Leaks: The Return of Heap Feng Shui
- IE 11 0day & Windows 8.1 Exploit
- IE11 Sandbox Escapes Presentation
- Spartan 0day & Exploit
- Look Mom, I don't use Shellcode
- Windows 10 x64 edge 0day and exploit
- 1-Day Browser & Kernel Exploitation
- The Secret of ChakraCore: 10 Ways to Go Beyond the Edge
- From Out of Memory to Remote Code Execution
- Attacking WebKit Applications by exploiting memory corruption bugs
- CVE-2018-5129: Out-of-bounds write with malformed IPC messages
- it-sec catalog browser exploitation chapter
- ZDI-18-428: An MsEdge InfoLeak Story
- AsiaSecWest-2018-Chakra-vulnerability-and-exploit-bypass-all-system-mitigation
- IE 0day Analysis And Exploit
- Attacking Client-Side JIT Compilers v2
- The Return of the JIT Part 1
- The Return of the JIT Part 2
- Using the JIT vulnerability to Pwning Microsoft Edge
- From Assembly to JavaScript and Back
- Exploiting CVE-2020-0041 - Part 1: Escaping the Chrome Sandbox
- Exploiting CVE-2020-0041 - Part 2: Escalating to root

### ↑ Mitigation Bypass

- Disarming EMET v5.0
- Disarming and Bypassing EMET 5.1
- Universal DEP/ASLR bypass with msucr71.dll and mona.py
- Chaining DEP with ROP – the Rubik’s[TM] Cube
- Bypassing Stack Cookies, SafeSeh, SEHOP, HW DEP and ASLR
- Development of a new Windows 10 KASLR Bypass (in One WinDBG Command)
- Disarming Enhanced Mitigation Experience Toolkit (EMET)
- Simple EMET EAF bypass
- Exploit Dev 101: Bypassing ASLR on Windows
- Bypassing Control Flow Guard in Windows 10
- Bypassing Control Flow Guard in Windows 10 - Part II
- BYPASS CONTROL FLOW GUARD COMPREHENSIVELY
- CROSS THE WALL-BYPASS ALL MODERN MITIGATIONS OF MICROSOFT EDGE
- How to find the vulnerability to bypass the Control Flow Guard
- Bypassing Memory Mitigation Using Data-Only Exploitation Technique
- CHAKRA JIT CFG BYPASS
- SMEP: What is it, and how to beat it on Windows
- ROP for SMEP bypass
- HEVD Exploits – Windows 10 x64 Stack Overflow SMEP Bypass
- HEVD: kASLR + SMEP Bypass
- Smashing The Browser
- Browser security mitigations against memory corruption vulnerabilities

### ↑ Kernel

- Windows Kernel Pool Spraying
- Windows Kernel Exploitation Basics - Part 1 : Introduction to DVWDDriver
- Windows Kernel Exploitation Basics - Part 2 : Arbitrary Memory Overwrite exploitation using HalDispatchTable
- Windows Kernel Exploitation Basics - Part 3 : Arbitrary Memory Overwrite exploitation using LDT
- Windows Kernel Exploitation Basics - Part 4 : Stack-based Buffer Overflow exploitation (bypassing cookie)
- Arbitrary Write primitive in Windows kernel (HEVD)
- MS11-080 Exploit – A Voyage into Ring Zero
- Windows kernel pool spraying fun - Part 1 - Determine kernel object size
- Windows kernel pool spraying fun - Part 2 - More objects
- Windows kernel pool spraying fun - Part 3 - Let's make holes
- Fuzzy Security - Kernel Exploitation -> Stack Overflow
- Fuzzy Security - Kernel Exploitation -> Write-What-Where
- Fuzzy Security - Kernel Exploitation -> Null Pointer Dereference
- Fuzzy Security - Kernel Exploitation -> Uninitialized Stack Variable
- Fuzzy Security - Kernel Exploitation -> Integer Overflow
- Fuzzy Security - Kernel Exploitation -> UAF
- Fuzzy Security - Kernel Exploitation -> Pool Overflow
- Fuzzy Security - Kernel Exploitation -> GDI Bitmap Abuse (Win7-10 32/64bit)
- Fuzzy Security - Kernel Exploitation -> RS2 Bitmap Necromancy
- Fuzzy Security - Kernel Exploitation -> Logic bugs in Razer rzpnk.sys
- Intro to Windows kernel exploitation 1/N: Kernel Debugging
- Intro to Windows kernel exploitation 2/N: HackSys Extremely Vulnerable Driver
- Intro to Windows kernel exploitation 3/N: My first Driver exploit
- Intro to Windows kernel exploitation 3.5/N: A bit more of the HackSys Driver
- Sharks in the Pool.: Mixed Object Exploitation in the Windows Kernel Pool
- Windows Kernel Exploitation Tutorial Part 1: Setting up the Environment
- Windows Kernel Exploitation Tutorial Part 2: Stack Overflow
- Windows Kernel Exploitation Tutorial Part 3: Arbitrary Memory Overwrite (Write-What-Where)
- Windows Kernel Exploitation Tutorial Part 4: Pool Feng-Shui → Pool Overflow
- Windows Kernel Exploitation Tutorial Part 5: NULL Pointer Dereference
- Windows Kernel Exploitation Tutorial Part 6: Uninitialized Stack Variable
- Windows Kernel Exploitation Tutorial Part 7: Uninitialized Heap Variable
- Windows Kernel Exploitation Tutorial Part 8: Use After Free
- Corelan Team (corelanc0d3r) Heap Spraying Demystified
- abatchy Kernel Exploitation 1: Setting up the environment
- abatchy Kernel Exploitation 2: Payloads
- abatchy Kernel Exploitation 3: Stack Buffer Overflow (Windows 7 x86/x64)
- abatchy Kernel Exploitation 4: Stack Buffer Overflow (SMEP Bypass)
- abatchy Kernel Exploitation 5: Integer Overflow
- abatchy Kernel Exploitation 6: NULL pointer dereference
- abatchy Kernel Exploitation 7: Arbitrary Overwrite (Win7 x86)
- Kernel Hacking With HEVD Part 1 - The Setup
- Kernel Hacking With HEVD Part 2 - The Bug
- Kernel Hacking With HEVD Part 3 - The Shellcode
- Kernel Hacking With HEVD Part 4 - The Exploit
- Kernel Hacking With HEVD Part 5 - The SMEP Version
- The Path to Ring-0 Windows Edition
- DIRECTX TO THE KERNEL
- Windows Kernel Graphics Driver Attack Surface
- Root Cause of the Kernel Privilege Escalation Vulnerabilities CVE-2019-0808
- Kernel Pool Overflow Exploitation In Real World – Windows 10
- Kernel Pool Overflow Exploitation In Real World – Windows 7
- Windows Kernel Exploitation - Exploiting HEVD x64 Use-After-Free using Generic Non-Paged Pool Feng-Shui
- Windows Kernel Exploitation Part 1: Stack Buffer Overflows
- Windows Kernel Exploitation Part 2: Type Confusion
- Windows Kernel Exploitation Part 3: Integer Overflow

### ↑ Misc

- Root Cause Analysis – Memory Corruption Vulnerabilities
- Windows 10 x86/wow64 Userland heap

#### About

List of Awesome Advanced Windows Exploitation References

- 📖 Readme
- 📄 GPL-3.0 license
- ☆ 1.3k stars
- 👁 65 watching
- 🍴 319 forks

#### Releases

No releases published

#### Packages

No packages published

#### Contributors 2

-  yeyintminthuhtut r0lan
-  GorZ3rk 飘落的枫月