















master
Go to file
Code

 0xDivyanshu-new Fix the sizeof to avoid casting in...  536d271 · 2 months ago  171 Commits		
 Builder	FIX: Normalized line ending of all files. ...	2 years ago
 Driver	Fix the sizeof to avoid casting into 64 b...	2 months ago
 Exploit	FIX: Updated copyright information	last year
 Screenshots	FIX: Added HEVD linux screenshots	last year
 Tools	FIX: fixed related to SMAP and added t...	last year
 Whitepaper	Black Hat Asia Arsenal 2016	8 years ago
 .gitignore	Added Linux port of ArbitraryWrite vul...	5 years ago
 CONTRIBUTING.md	FIX: Normalized line ending of all files. ...	2 years ago
 LICENSE	FIX: Github is not parsing LICENSE file ...	2 years ago
 README.md	FIX: Added new blogposts and discord ...	last year
 appveyor.yml	ENHANCEMENT: Updated appveyor co...	5 years ago

[illegible]

About

HackSys Extreme Vulnerable Driver (HEVD) - Windows & Linux


hacksys.io

-
- A word cloud of security-related terms in light blue rounded rectangles. The terms are: windows, linux, kernel, driver, vulnerabilities, exploitation, uaf, buffer-overflow, memory-corruption, exploit-development, hevd, info-leak, and type-confusion.

-  Readme
-  GPL-3.0 license
-  Activity
-  2.5k stars
-  97 watching
-  532 forks

Report repository

Releases 3

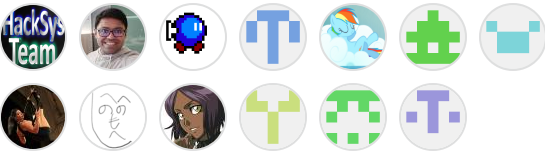
 **HEVD v3.00** Latest
on Jun 28, 2019

+ 2 releases

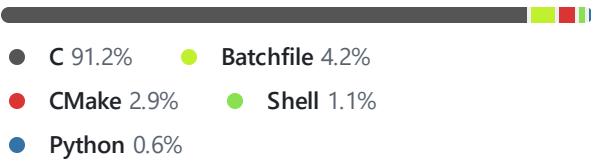
Packages

No packages published

Contributors 13



Languages



- [Presentation](#)
- [White Paper](#)

Blog Post

- <http://www.payatu.com/hacksys-extreme-vulnerable-driver/>

External Exploits

- <https://github.com/sam-b/HackSysDriverExploits>
- <https://github.com/sizzop/HEVD-Exploits>
- <https://github.com/badd1e/bug-free-adventure>
- <https://github.com/FuzzySecurity/HackSysTeam-PSKernelPwn>
- <https://github.com/theevilbit/exploits/tree/master/HEVD>
- <https://github.com/GradiusX/HEVD-Python-Solutions>
- <http://pastebin.com/ALKdpDsF>
- <https://github.com/Cn33liz/HSEVD-StackOverflow>
- <https://github.com/Cn33liz/HSEVD-StackOverflowX64>
- <https://github.com/Cn33liz/HSEVD-StackCookieBypass>
- <https://github.com/Cn33liz/HSEVD-ArbitraryOverwrite>
- <https://github.com/Cn33liz/HSEVD-ArbitraryOverwriteGDI>
- <https://github.com/Cn33liz/HSEVD-StackOverflowGDI>
- <https://github.com/Cn33liz/HSEVD-ArbitraryOverwriteLowIL>
- https://github.com/mgeeky/HEVD_Kernel_Exploit
- <https://github.com/tekwizz123/HEVD-Exploit-Solutions>
- <https://github.com/FULLSHADE/Windows-Kernel-Exploitation-HEVD>
- https://github.com/w4fz5uck5/3XPL01t5/tree/master/OSEE_Training

External Blog Posts

- <http://niiconsulting.com/checkmate/2016/01/windows-kernel-exploitation/>
- http://samdb.xyz/2016/01/16/intro_to_kernel_exploitation_part_0.html
- http://samdb.xyz/2016/01/17/intro_to_kernel_exploitation_part_1.html
- http://samdb.xyz/2016/01/18/intro_to_kernel_exploitation_part_2.html
- http://samdb.xyz/2017/06/22/intro_to_kernel_exploitation_part_3.html
- <https://sizzop.github.io/2016/07/05/kernel-hacking-with-hevd-part-1.html>
- <https://sizzop.github.io/2016/07/06/kernel-hacking-with-hevd-part-2.html>
- <https://sizzop.github.io/2016/07/07/kernel-hacking-with-hevd-part-3.html>
- <https://sizzop.github.io/2016/07/08/kernel-hacking-with-hevd-part-4.html>
- <https://www.fuzzysecurity.com/tutorials/expDev/14.html>
- <https://www.fuzzysecurity.com/tutorials/expDev/15.html>
- <https://www.fuzzysecurity.com/tutorials/expDev/16.html>
- <https://www.fuzzysecurity.com/tutorials/expDev/17.html>
- <https://www.fuzzysecurity.com/tutorials/expDev/18.html>
- <https://www.fuzzysecurity.com/tutorials/expDev/19.html>
- <https://www.fuzzysecurity.com/tutorials/expDev/20.html>
- <http://dokydoky.tistory.com/445>
- <https://hshrzd.wordpress.com/2017/05/28/starting-with-windows-kernel-exploitation-part-1-setting-up-the-lab/>
- <https://hshrzd.wordpress.com/2017/06/05/starting-with-windows-kernel-exploitation-part-2/>
- <https://hshrzd.wordpress.com/2017/06/22/starting-with-windows-kernel-exploitation-part-3-stealing-the-access-token/>
- <https://osandamalith.com/2017/04/05/windows-kernel-exploitation-stack-overflow/>

- <https://osandamalith.com/2017/06/14/windows-kernel-exploitation-arbitrary-overwrite/>
- <https://osandamalith.com/2017/06/22/windows-kernel-exploitation-null-pointer-dereference/>
- <http://dali-mrabet1.rhcloud.com/windows-kernel-exploitation-arbitrary-memory-overwrite-hevd-challenges/>
- <https://blahcat.github.io/2017/08/31/arbitrary-write-primitive-in-windows-kernel-hevd/>
- https://klue.github.io/blog/2017/09/hevd_stack_gs/
- <https://glennmcgui.re/introduction-to-windows-kernel-exploitation-pt-1/>
- <https://glennmcgui.re/introduction-to-windows-kernel-driver-exploitation-pt-2/>
- https://kristal-g.github.io/2021/02/07/HEVD_StackOverflowGS_Windows_10_RS5_x64.html
- https://kristal-g.github.io/2021/02/20/HEVD_Type_Confusion_Windows_10_RS5_x64.html
- <https://wafzsucks.medium.com/hacksys-extreme-vulnerable-driver-arbitrary-write-null-new-solution-7d45bfe6d116>
- <https://wafzsucks.medium.com/how-a-simple-k-typeconfusion-took-me-3-months-long-to-create-a-exploit-f643c94d445f>
- <https://mdanilor.github.io/posts/hevd-0/>
- <https://mdanilor.github.io/posts/hevd-1/>
- <https://mdanilor.github.io/posts/hevd-2/>
- <https://mdanilor.github.io/posts/hevd-3/>
- <https://mdanilor.github.io/posts/hevd-4/>

Author

Ashfaq Ansari

ashfaq[at]hacksys[dot]io

[Blog](#) |
 [@HackSysTeam](#)



<https://hacksys.io/>

Screenshots

```

##      ## #####  ##      ## #####
##      ##  ##      ##      ##  ##      ##
##      ##  ##      ##      ##  ##      ##
#####  #####  ##      ##  ##      ##
##      ##  ##      ##      ##  ##      ##
##      ##  ##      ##      ##  ##      ##
##      ## #####  ##      ## #####
HackSys Extreme Vulnerable Driver

```

```

    ##      ## ##### ##      ## #####
    ##      ## ##      ##      ## ##
    ##      ## ##      ##      ## ##
    ##### ## #####      ##      ##
    ##      ## ##      ##      ## ##
    ##      ## ##      ##      ## ##
    ##      ## #####      ## #####

HackSys Extreme Vulnerable Driver Exploits
Ashfaq Ansari (@HackSysTeam)
ashfaq[at]payatu[dot]lcom

Usage: HackSysEVDExploit.exe [option] -c [process to launch]

HackSysEVDExploit.exe -a cmd.exe

[option]
-p : Pool Overflow
-s : Stack Overflow
-u : Use After Free
-t : Type Confusion
-i : Integer Overflow
-g : Stack Overflow GS
-n : Null Pointer Dereference
-a : Arbitrary Memory Overwrite

```

```

C:\Windows\system32\cmd.exe - HackSysEVDExploit.exe -p -c cmd.exe

    ##      ## ##### ##      ## #####
    ##      ## ##      ##      ## ##
    ##      ## ##      ##      ## ##
    ##### ## #####      ##      ##
    ##      ## ##      ##      ## ##
    ##      ## ##      ##      ## ##
    ##      ## #####      ## #####

HackSys Extreme Vulnerable Driver Exploits
Ashfaq Ansari (@HackSysTeam)
ashfaq[at]payatu[dot]lcom

[+] Starting Pool Overflow Exploitation
[+] Creating The Exploit Thread
[+] Exploit Thread Handle: 0x50
[+] Setting Thread Priority
[+] Priority Set To THREAD_PRIORITY_HIGHEST
[+] Getting Device Driver Handle
[+] Device Name: \\.\HackSysExtremeVulnerableDriver
[+] Device Handle: 0x54
[+] Setting Up Vulnerability Stage
[+] Allocating Memory For Buffer
[+] Memory Allocated: 0x00480D18
[+] Allocation Size: 0x220
[+] Mapping Null Page
[+] Memory Allocated: 0x00000000
[+] Allocation Size: 0x2000
[+] Preparing Buffer Memory Layout
[+] TypeIndex Of Event Object Set To: 0x0
[+] Preparing OBJECT_TYPE At Null Page
[+] DeleteProcedure Value: 0x1132770
[+] DeleteProcedure Address: 0x00000060
[+] EoP Payload: 0x01132770
[+] Preparing NonPaged Kernel Pool Layout
[+] Spraying With Event Objects
[+] Creating Holes By Coalescing
[+] Triggering Pool Overflow
[+] Triggering Payload
[+] Freeing Event Objects
[+] Completed Pool Overflow Exploitation
[+] Checking Current Process Privileges
[+] Trying To Get Process ID Of: csrss.exe
[+] Process ID Of csrss.exe: 344
[+] Trying To Open csrss.exe With PROCESS_ALL_ACCESS
[+] Process Handle Of csrss.exe: 0xEB08
[+] Successfully Elevated Current Process Privileges
[+] Enjoy As SYSTEM [0.000000]s

```

```

kd> g
***** HACKSYS_EVD_IOCTL_POOL_OVERFLOW *****
[+] Allocating Pool Buffer
[+] Pool Address: 0x84AC7448
[+] Pool Type: NonPagedPool
[+] Pool Size: 0x1F8
[+] Pool Tag: 'kcaH'
[+] pUserModeBuffer: 0x001F0D18
[+] userModeBufferSize: 0x220
[+] Triggering Pool Overflow
[+] Freeing Pool Memory
[+] Pool Address: 0x84AC7448
[+] Pool Tag: 'kcaH'
***** HACKSYS_EVD_IOCTL_POOL_OVERFLOW *****

```

Vulnerabilities Implemented

- Write NULL
- Double Fetch
- Buffer Overflow
 - Stack
 - Stack GS
 - NonPagedPool
 - NonPagedPoolNx
 - PagedPoolSession
- Use After Free
 - NonPagedPool

- NonPagedPoolNx
- Type Confusion
- Integer Overflow
 - Arithmetic Overflow
- Memory Disclosure
 - NonPagedPool
 - NonPagedPoolNx
- Arbitrary Increment
- Arbitrary Overwrite
- Null Pointer Dereference
- Uninitialized Memory
 - Stack
 - NonPagedPool
- Insecure Kernel Resource Access

Building the driver

- [Install Visual Studio 2017](#)
- [Install Windows Driver Kit](#)
- Run the appropriate driver builder `Build_HEVD_Vulnerable_x86.bat` or `Build_HEVD_Vulnerable_x64.bat`

Download

If you do not want to build **HackSys Extreme Vulnerable Driver** from source, you could download pre-built executables for the latest release:

<https://github.com/hacksystem/HackSysExtremeVulnerableDriver/releases>

Installing the driver

Use [OSR Driver Loader](#) to install **HackSys Extreme Vulnerable Driver**

Testing

The **HackSys Extreme Vulnerable Driver** and the respective exploits have been tested on **Windows 7 SP1 x86** and **Windows 10 x64**

Sessions Conducted

- [Windows Kernel Exploitation 1](#)
- [Windows Kernel Exploitation 2](#)
- [Windows Kernel Exploitation 3](#)
- [Windows Kernel Exploitation 4](#)
- [Windows Kernel Exploitation 5](#)
- [Windows Kernel Exploitation 6](#)
- [Windows Kernel Exploitation 7](#)

Workshops Conducted

- [Windows Kernel Exploitation Humla Pune](#)
- [Windows Kernel Exploitation Humla Mumbai](#)

HEVD for Linux

```
[ 8252.362862] hevd:
      ##      ## ##### ##      ## #####
      ##      ## ##      ##      ## ##      ##
      ##      ## ##      ##      ## ##      ##
      ##### #####      ##      ## ##      ##
      ##      ## ##      ##      ## ##      ##
      ##      ## ##      ## ##      ##      ##
      ##      ## #####      ##      #####
      HackSys Extreme Vulnerable Driver
      Version: 4.00
[ 8252.362864] hevd: [+] HackSys Extreme Vulnerable Driver Loaded
```

```
osboxes@osboxes:~/Desktop/HackSysExtremeVulnerableDriver/Tools$ sudo bash hevd_linux_installer.sh install
✓ Kernel module loaded successfully
🔒 Permissions updated: /dev/HackSysExtremeVulnerableDriver
osboxes@osboxes:~/Desktop/HackSysExtremeVulnerableDriver/Tools$ sudo bash hevd_linux_installer.sh uninstall
✓ Kernel module unloaded successfully
```

```
🏆 HackSys Extreme Vulnerable Driver (HEVD) - Linux 🏆

🚀 Triggering: HEVD_IOCTL_BUFFER_OVERFLOW_STACK - 0xC0206800
    ● Input buffer: 0x21153D0
    ● Input buffer length: 0x1000
✓ IOCTL executed successfully!

🚀 Triggering: HEVD_IOCTL_INTEGER_OVERFLOW - 0xC0206809
    ● Input buffer: 0x21143A0
    ● Input buffer length: 0x800
✓ IOCTL executed successfully!
```

```
[10675.661165] hevd: ***** HEVD_IOCTL_BUFFER_OVERFLOW_STACK *****
[10675.661167] hevd: [+] user_buffer: 0x0000000040067bf3
[10675.661167] hevd: [+] user_buffer size: 0x1000
[10675.661168] hevd: [+] kernel_buffer: 0x000000004d8654df
[10675.661168] hevd: [+] kernel_buffer size: 0x1000
[10675.661168] hevd: [+] Triggering Buffer Overflow in Stack
[10675.661169] hevd: ***** HEVD_IOCTL_BUFFER_OVERFLOW_STACK *****
[10675.661210] hevd: ***** HEVD_IOCTL_INTEGER_OVERFLOW *****
[10675.661211] hevd: [+] user_buffer: 0x0000000012d259ed
[10675.661211] hevd: [+] user_buffer size: 0x800
[10675.661211] hevd: [+] kernel_buffer: 0x00000000a3ed5874
[10675.661212] hevd: [+] kernel_buffer size: 0x1000
[10675.661212] hevd: [+] Triggering Integer Overflow
[10675.661216] hevd: ***** HEVD_IOCTL_INTEGER_OVERFLOW *****
```

License

Please see the file `LICENSE` for copying permission

Contribution Guidelines

Please see the file `CONTRIBUTING.md` for contribution guidelines

TODO & Bug Reports

Please file any enhancement request or bug report via the **GitHub** issue tracker at the below-given address:
<https://github.com/hacksystem/HackSysExtremeVulnerableDriver/issues>

Acknowledgments

Thanks go to these wonderful people: 🇺🇸

