Use After Free Vulnerabilities

Software Security 2019/2020

Andrea Lanzi

Use After Free Vulnerability

- Use-after-free vulnerabilities are **very hard to spot during manual code review** as they require knowing the pattern of allocation and deallocation that occurs during a program's execution
- The vulnerability is a **temporary** one, that only exists at particular points in time when the stale pointer presents itself.

CVE-2017-5031 : A **use after free** in ANGLE in Google **Chrome** prior ...
www.cvedetails.com/cve/CVE-2017-5031/
May 8, 2017 ... CVE-2017-5031 : A **use after free** in ANGLE in Google **Chrome** prior to 57.0. 2987.98 for Windows allowed a remote attacker to perform an out ...

CVE-2013-6621 : **Use-after-free** vulnerability in Google **Chrome** ...
www.cvedetails.com/cve/CVE-2013-6621/
Sep 21, 2016 ... **Use-after-free** vulnerability in Google **Chrome** before 31.0.1650.48 allows remote attackers to cause a denial of service or possibly have ...

CVE-2013-2870 : **Use-after-free** vulnerability in Google **Chrome** ...
www.cvedetails.com/cve/CVE-2013-2870/
Oct 18, 2016 ... **Use-after-free** vulnerability in Google **Chrome** before 28.0.1500.71 allows remote servers to execute arbitrary code via crafted response traffic ...

CVE-2013-6625 : **Use-after-free** vulnerability in core/dom ...
www.cvedetails.com/cve/CVE-2013-6625/
Dec 7, 2016 ... **Use-after-free** vulnerability in core/dom/ContainerNode.cpp in Blink, as used in Google **Chrome** before 31.0.1650.48, allows remote attackers ...

CVE-2012-5140 : **Use-after-free** vulnerability in Google **Chrome** ...
www.cvedetails.com/cve/CVE-2012-5140/
Sep 28, 2016 ... **Use-after-free** vulnerability in Google **Chrome** before 23.0.1271.97 allows remote attackers to cause a denial of service or possibly have ...

CVE-2013-2885 : **Use-after-free** vulnerability in Google **Chrome** ...
www.cvedetails.com/cve/CVE-2013-2885/
Oct 18, 2016 ... **Use-after-free** vulnerability in Google **Chrome** before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have ...

CVE-2012-5139 : **Use-after-free** vulnerability in Google **Chrome** ...
www.cvedetails.com/cve/CVE-2012-5139/
Sep 28, 2016 ... **Use-after-free** vulnerability in Google **Chrome** before 23.0.1271.97 allows remote attackers to cause a denial of service or possibly have ...

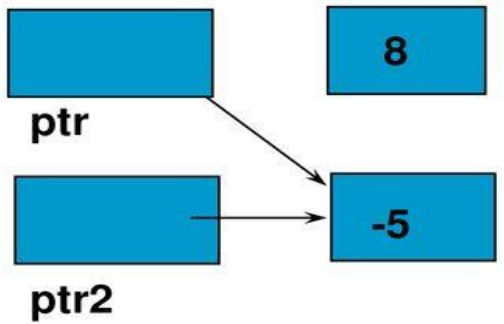
Use After Free Vulnerability

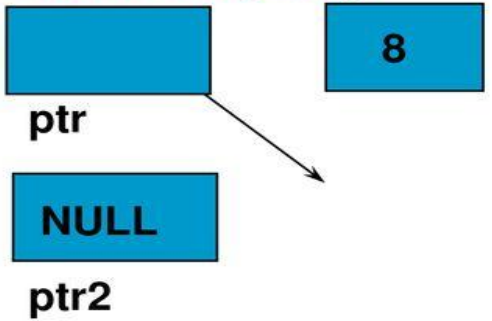
- **Use-after-free** vulnerability happens when a pointer to an object that has been freed is deferenced.
- This can result in information leakage but the attacker could also modify an unintended memory locations that **potentially can lead to code execution**.

Leaving a Dangling Pointer

```
int* ptr = new int;
*ptr = 8;
int* ptr2 = new int;
*ptr2 = -5;
ptr = ptr2;

delete ptr2;      // ptr is left dangling
ptr2 = NULL;
```





Example of Use After Free Vulnerability

```
char *retptr() {

char p ,*q ;
q = &p ;

return q ; /* deallocation on the stack */

}
```

```
int main( ){

    char *a , *b;
    int i ;

    a = malloc(16) ;
    b = a + 5;

    free(a) ;
    b[2] = 'c' ; /* use after free */

    b = retptr( ) ;
    *b = 'c' ;    /* use after free */

}
```

Exploitable Example of Use After Free

https://github.com/andrealan/Software-Security-Lab/blob/master/uaf-exercise/uaf-example.c