

Forum:[Hack Forums](#)

Thread: [\[CVE-2024-9680\] Explaining the Firefox 0Day that abuses use-after-free](#)

Biggy_Asian - October 18, 2024, 5:35 am

The firefox/tor browser is vulnerable on some versions by abusing a `use-after-free` vulnerability. This does not make CSS harmful however it is just an exploit within the handling of CSS within the Mozilla browser.

The way it could be exploited is through a method like type confusion.

This can happen when you have a pointer -> you free(MyPTR) -> you didnt clean it up correctly so it still exists which then can be used as a spot for an RCE.

So like this: myPTR -> free(myPTR) -> myPTR still exists and is waiting for some new data -> attacker sets myPTR -> AttackerShell() -> myPTR gets executed which in turn runs the AttackerShell() function instead.

This pretty much works by confusing the engine making it think your a foo and bar which then means the engine will get a type confusion error.

This causes the structure values to then overlap with each other.

If the attacker can control the Identifier then then they have a potential RCE vulnerability as they can control the ptr which gets executed below in the "out" input.

TLDR: Confuse the browser by making it think its two different things which then causes a type confusion error which can then be exploited and if exploited the attacker can drop and run their payload into your memory which then gets executed by a trusted process like your browser.

Here is an example of some vulnerable C/C++ code:

[The following code is pretty much just copied from Low Level](#)

Code // I wrote this shit in the browser dont mind the formatting.

```
// same structures, different name and flipped structure.
```

```
struct foo {  
    int Identity;  
    void (*ptr)(int); // we will set the function below which will be called later  
}
```

```
struct bar {  
    void (*ptr)(int); // we will set the function below which will be called later  
    int Identity;  
}
```

```
// defining our structures so we can actually utilize them
```

```
struct foo *fooS;  
struct bar *barS;
```

```
void Foo_Out(int id){  
    printf("Foo");  
}
```

```
void Bar_Out(int id){  
    printf("Bar");  
}
```

// how we will use the defined code above.

```
int main() {  
    char buffer[32];  
  
    while (buffer[0] != 'q') {  
        scanf('%32s', buff);  
  
        // type checking for input  
  
        if (!strcmp(buff, "NewFoo")) {  
            fooS = malloc(sizeof(struct foo)); // we memory allocate (malloc) and the sizeof it will be the  
structure  
            fooS->ptr = Foo_Out; // set the function ptr to Foo_Out as we will want to use this later  
            fooS->Identity = 0x4242424242424242; // random address  
        } else if (!strcmp(buff, "NewBar")) {  
            barS = malloc(sizeof(struct bar)); // we memory allocate (malloc) and the sizeof it will be the  
structure  
            barS->ptr = Bar_Out; // set the function ptr to Bar_Out as we will want to use this later  
            barS->Identity = 0x4141414141414141; // random address  
        } else if (!strcmp(buff, "DelFoo")) {  
            free(fooS); // bad by its self because we can ref the function pointer later because it dangles  
            // can fix by doing barS = NULL; lol  
        } else if (!strcmp(buff, "DelBar")) {  
            free(barS); // bad by its self because we can ref the function pointer later because it dangles  
            // can fix by doing barS = NULL; lol  
        } else if (!strcmp(buff, "out")) {  
            fooS->ptr(0); // execute the print function  
            barS->ptr(0); // execute the print function  
        }  
    }  
}
```

Exploitable versions UPDATE ASAP:

Sources:

<https://nvd.nist.gov/vuln/detail/CVE-2024-9680>

<https://www.msn.com/en-us/money/other/update-firefox-131-now-to-patch-a-critical-zero-day-security-flaw/ar-AA1s2kNk>

For others just use google <3

InspectorGadget - October 18, 2024, 5:43 am

Nice thread mate.

Known affected versions:

Also here's a better source:

<https://nvd.nist.gov/vuln/detail/CVE-2024-9680>

Biggy_Asian - *October 18, 2024, 5:45 am*

(Oct 18, 2024 05:43 AM)InspectorGadget Wrote: [\[CITE\]](#) Nice thread mate.

Known affected versions:

Also here's a better source:

<https://nvd.nist.gov/vuln/detail/CVE-2024-9680>

Appreciate it. Ill add the sources to the thread now <3