# Chrome 远程代码执行0Day漏洞

## 脆弱性评价

| 威胁级别 | 严重 | ■ | 中度 |  | 轻度 |  |
| --- | --- | --- | --- | --- | --- | --- |

## 漏洞危害

国外安全研究员发布了Chrome 远程代码执行 0Day漏洞的POC（概念验证代码）详情，漏洞等级“严重”级别。攻击者利用此漏洞，构造一个恶意的web页面，用户访问该页面时，会造成远程代码执行。

该0day漏洞已被验证，目前Google只针对该漏洞发布了beta测试版Chrome（90.0.4430.70）修复，Chrome正式版（ 89.0.4389.114）仍受漏洞影响。

## 详细信息

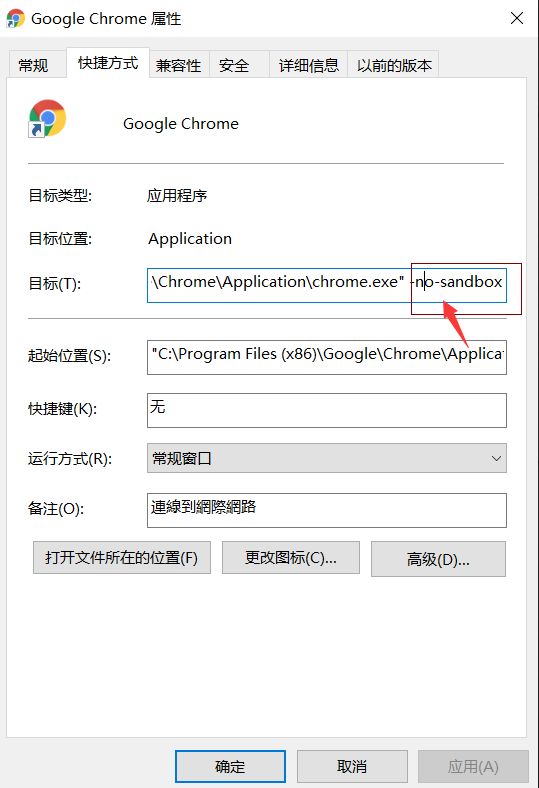
chrome历史版本下载：

https://sourceforge.net/projects/portableapps/files/Google%20Chrome%20Portable/

https://www.chromium.org/getting-involved/dev-channel（需要翻墙）

测试需求：关闭沙箱环境 (目前已泄露的exp需关闭沙箱环境才可执行)

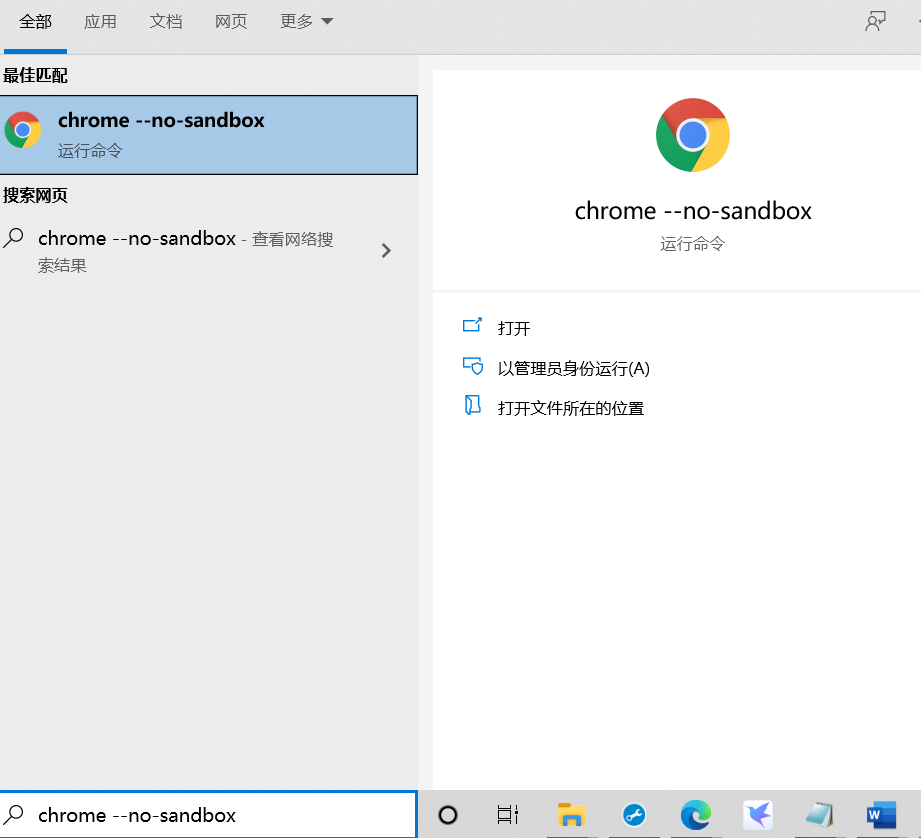
1、关闭chrome沙箱 快捷键>>浏览器>>属性>>目标 切记路径后4个空格然后跟上 no-sandbox



或者用文件资源器中访问。

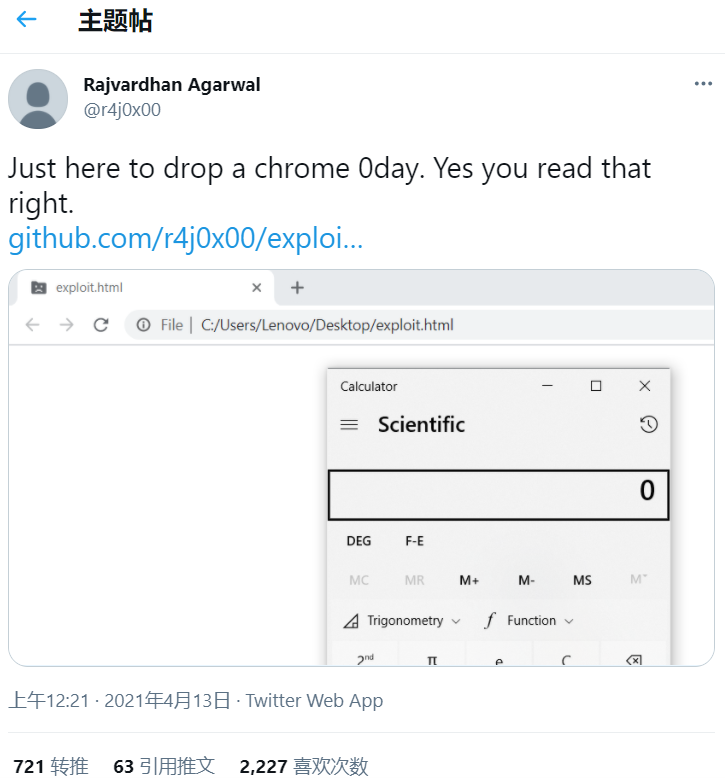
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe -no-sandbox

或者在查询框运行命令关闭沙箱



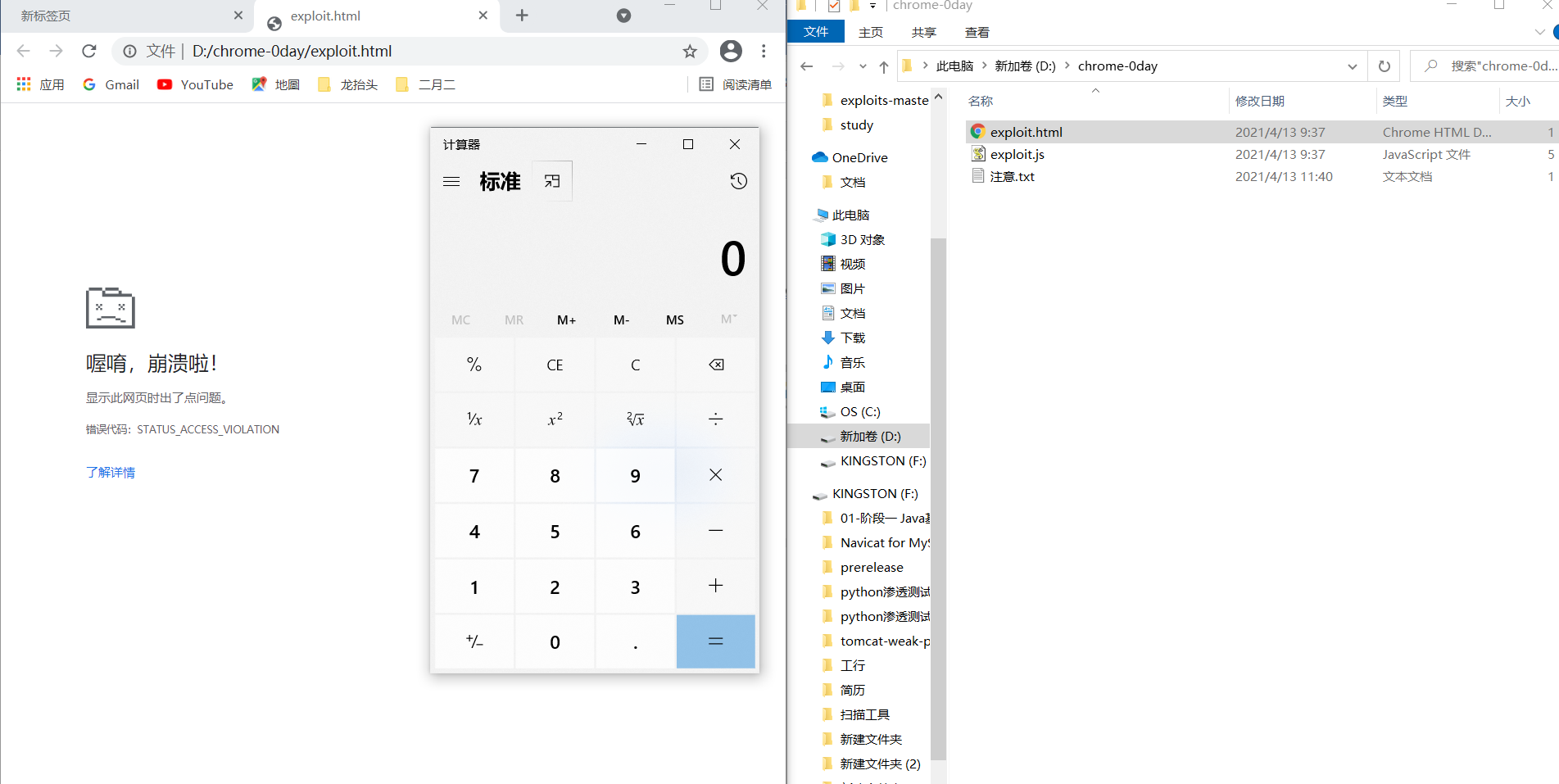
2、下载exp，360cert参考链接上推特上的exp github地址

<https://github.com/r4j0x00/exploits/tree/master/chrome-0day>



3、exp演示

在已关闭沙箱的chrome里打开exploit.html，exploit.html会加载exploit.js



成功执行calc命令，弹出计算器框。

## 修复建议

1、更新至beta测试版Chrome（90.0.4430.70）。  
        2、不要以非沙箱模式运行chrome。

## 参考链接

<https://twitter.com/r4j0x00/status/1381643526010597380>  
        <https://mp.weixin.qq.com/s/qlw01wjJ0iIQUNgGYQrlMA>