安全漏洞通告

【POC 公开】Chrome 远程代码执行 0Day 漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-04-13

报告信息

报告名称	【POC 公开】Chrome 远程代码执行 0Day 漏洞通告		
报告类型	安全漏洞通告	**报告编号**	B6-2021-041301
报告版本	1	**报告日期**	2021-04-13
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-04-13	360CERT	360CERT	撰写报告

目录

一、 漏洞档案

漏洞类型	命令执行
CVE 编号	暂无
相关厂商	google
相关组件	Chrome
威胁等级	严重
影响面	广泛
360CERT 评分	9.8
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2021-04-13
报告生成时间	2021-04-13

二、 漏洞简述

2021 年 04 月 13 日，360CERT 监测发现 国外安全研究员 发布了 Chrome 远程代码执行 0Day 的 POC 详情，漏洞等级：严重，漏洞评分：9.8。

Google Chrome 是由 Google 开发的免费网页浏览器。Chrome 是化学元素“铬”的英文名称，过去也用 Chrome 称呼浏览器的外框。Chrome 相应的开放源代码计划名为 Chromium，而 Google Chrome 本身是非自由软件，未开放全部源代码。

该漏洞已验证，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）仍存在漏洞，360CERT 建议广大用户关注官方 Chrome 正式版更新，及时修补漏洞。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

三、 漏洞评级

经过安全技术人员的分析，最终对该漏洞的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	9.8

四、 漏洞详情

Chrome 远程代码执行漏洞

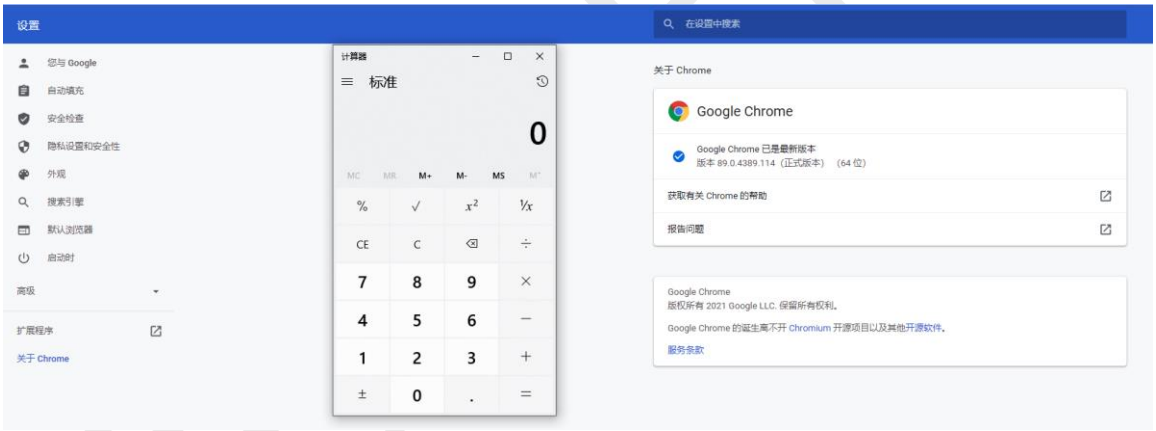
组件: Chrome

漏洞类型: 命令执行

影响: 服务器接管

简述: 攻击者利用此漏洞，可以构造一个恶意的 web 页面，当用户访问该页面时，会造成远程代码执行。

目前该漏洞已在最新版本 Chrome 上得到验证



五、 影响版本

产品名称	影响版本
Google:Chrome	<=89.0.4389.114

六、 漏洞列表

编号	描述	导致结果	威胁等级
暂无	命令执行	服务器接管	严重

七、 安全建议

(一) 通用修补方案

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）仍存在漏洞，请关注官方 Chrome 正式版更新，及时修补漏洞。

(二) 临时修补方案

强烈建议广大用户在 SandBox 模式下运行 Chrome

八、 产品侧解决方案

(一) 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。

九、 参考链接

1. Stable Channel Update for Desktop

   https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_30.html

2. Researcher's Twitter

   https://twitter.com/r4j0x00/status/1381643526010597380

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 – 10.0	严重
7.0 – 8.9	高危
4.0 – 6.9	中危
0 - 3.9	低危