

安全漏洞通告

Chrome 安全问题可能导致 Windows 版微信任意代码执行漏洞通告

360CERT

北京奇虎科技有限公司 | 2021-04-19

报告信息

报告名称	Chrome 安全问题可能导致 Windows 版微信任意代码执行漏洞 通告		
报告类型	安全漏洞通告	报告编号	B6-2021-041701
报告版本	1	报告日期	2021-04-19
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	2021-04-19	360CERT	360CERT	撰写报告

目录

一、	漏洞档案	1
二、	漏洞简述	2
三、	漏洞评级	3
四、	漏洞详情	4
五、	影响版本	5
六、	漏洞列表	6
七、	安全建议	7
(一)	通用修补方案	7
八、	产品侧解决方案	8
(一)	360 安全卫士	8
(二)	360 本地安全大脑	8
(三)	360 终端安全管理系统	9
九、	参考链接	10
附录 A	报告风险等级说明	11
附录 B	影响面说明	13
附录 C	360 内部评分体系	14

一、漏洞档案



漏洞类型	代码执行
CVE 编号	暂无
相关厂商	tencent
相关组件	暂无
威胁等级	严重
影响面	广泛
360CERT 评分	8.8
修复方案	通用修补方案
漏洞发布时间	2021-04-17
报告生成时间	2021-04-19

二、漏洞简述

2021年04月17日，360CERT监测发现腾讯安全应急响应中心发布了关于Chrome存在安全问题可能影响Windows版本微信的风险通告，漏洞等级：严重，漏洞评分：8.8。

对此，360CERT建议广大用户及时将微信升级到最新版本。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。

360CERT

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	8.8

四、漏洞详情

Chrome 安全问题可能导致 Windows 版微信任意代码执行漏洞

组件: Windows 版微信

漏洞类型: 远程代码执行

影响: PC 接管

简述: 攻击者可以通过微信发送一个特制的 web 链接, 用户一旦点击链接, Windows 版微信便会加载执行攻击者构造恶意代码, 最终使攻击者控制用户 PC。

五、影响版本

产品名称	影响版本
tencnet:wechat	<=3.2.1.132

360CERT

六、 漏洞列表

编号	描述	导致结果	威胁等级
暂无	代码执行	服务器接管	严重

360CERT

七、安全建议

(一) 通用修补方案

目前微信已经修复漏洞并发布了更新版本，360CERT 强烈建议用户立即将 Windows 版微信更新到 3.2.1.141 以上的最新版本。

360CERT

八、产品侧解决方案

(一) 360 安全卫士

针对本次安全更新，Windows 用户可通过 360 安全卫士实现对应补丁安装，其他平台的用户可以根据修复建议列表中的产品更新版本对存在漏洞的产品进行更新。如有其他问题可联系相关产品负责人或（360safe-ent#360.cn）。



(二) 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。



(三) 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。



九、 参考链接

1. 腾讯安全应急响应中心安全通告

<https://mp.weixin.qq.com/s/qAnxwM1Udulj1K3Wn2awVQ>

2. 青藤云安全安全通告

<https://mp.weixin.qq.com/s/e6D-jLhkehr9AG4hu0LfwA>

360CERT

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	<ol style="list-style-type: none"> 1. $9.0 \leq 360\text{CERT 评分} \leq 10$ 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. $7.0 \leq 360\text{CERT 评分} < 9$ 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. $4.0 \leq 360\text{CERT 评分} < 7$ 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 <ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. $0 \leq 360\text{CERT 评分} < 4$ 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