奇安信
新一代网络安全领军者

钉钉电脑版远程代码执行漏洞

安全风险通告

奇安信 CERT

2022 年 02 月 17 日

目录

第1章 安全通告

尊敬的客户：

近日，奇安信 CERT 监测到钉钉电脑版远程代码执行漏洞 PoC 已在互联网上公开。攻击者可将恶意代码托管在服务器上，诱使受害者使用钉钉打开链接，钉钉即会获取恶意链接指向的网页内容并用内置浏览器渲染，从而触发漏洞，在受害者电脑上远程执行代码。目前，此漏洞已发现在野利用且 PoC 已公开，经奇安信安全团队验证，此 PoC 有效。鉴于此漏洞影响较大，建议用户尽快自查修复。

当前漏洞状态：

漏洞编号	威胁类型	漏洞威胁状态			
		技术细节状态	PoC状态	EXP状态	在野利用
QVD-2022-1438	代码执行	已公开	已公开	未知	已发现

奇安信 CERT 将持续关注该漏洞进展，并第一时间为您更新该漏洞信息。

第2章 文档信息

文档名称	钉钉电脑版远程代码执行漏洞安全风险通告
关键字	远程代码执行、在野利用
发布日期	2022 年 02 月 17 日
分析团队	奇安信 CERT

第3章 漏洞信息

3.1 漏洞描述

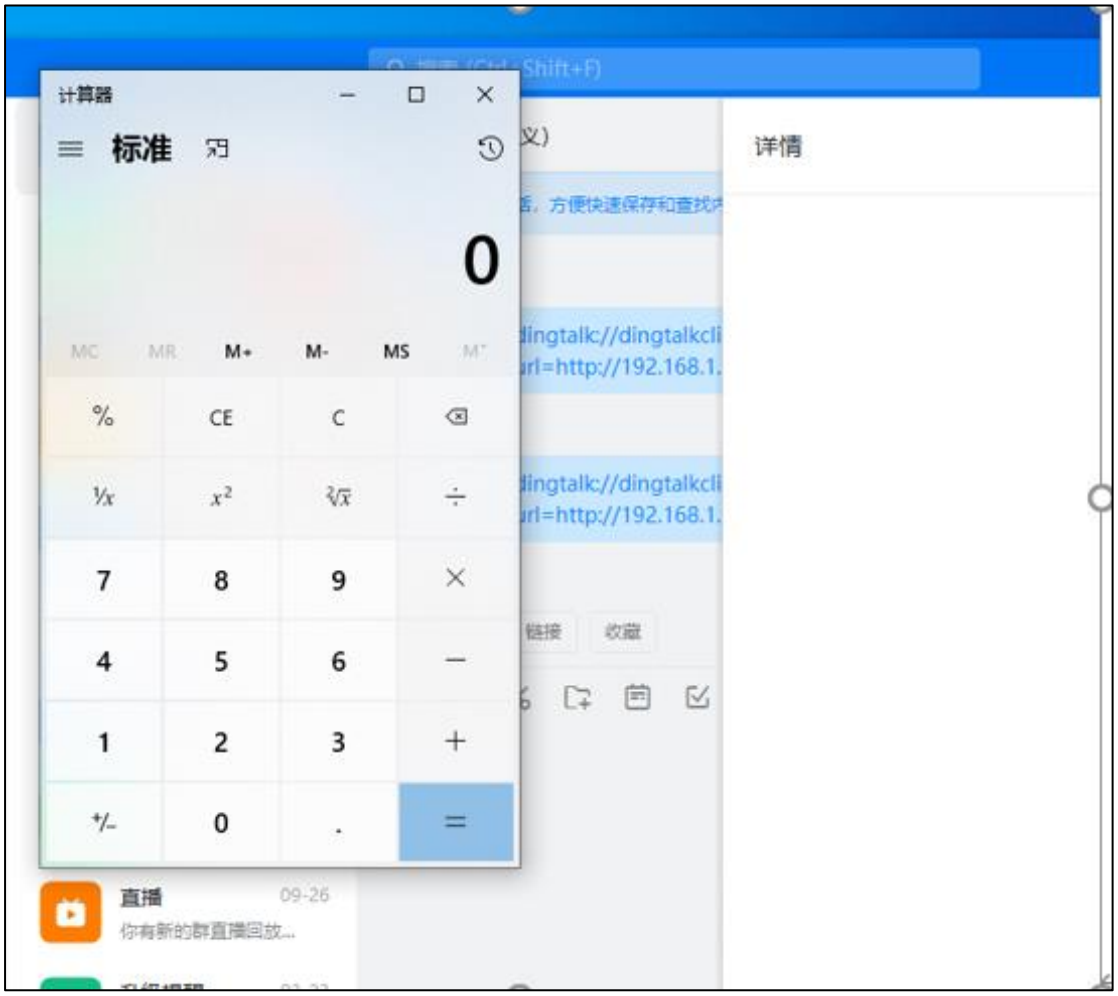
钉钉是阿里集团专为中小企业打造的通讯、协同的移动办公平台，提供 PC 版，Web 版，Mac 版和手机版，帮助企业更加高效安全地进行内部沟通和商务沟通。

近日，奇安信 CERT 监测到钉钉电脑版远程代码执行漏洞 PoC 已在互联网上公开。攻击者可将恶意代码托管在服务器上，诱使受害者使用钉钉打开链接，钉钉即会获取恶意链接指向的网页内容并用内置浏览器渲染，从而触发漏洞，在受害者电脑上远程执行代码。目前，此漏洞已发现在野利用且 PoC 已公开，经奇安信安全团队验证，此 PoC 有效。鉴于此漏洞影响较大，建议用户尽快自查修复。

QVD-2022-1438 钉钉电脑版远程代码执行漏洞

漏洞名称	钉钉电脑版远程代码执行漏洞				
漏洞类型	代码执行	**风险等级**	高危	**漏洞 ID**	QVD-2022-1438
公开状态	已公开	**在野利用**	已发现		
漏洞描述	钉钉电脑版中存在远程代码执行漏洞，远程攻击者可通过诱导用户使用钉钉打开特制链接来利用此漏洞，成功利用此漏洞的攻击者可在目标系统上执行任意代码。				
参考链接					
https://page.dingtalk.com/wow/z/dingtalk/default/dddownload-index					

奇安信安全团队已第一时间复现此漏洞，截图如下：



DingTalk.exe	1.12	107,460 K	139,152 K	6864 钉钉	Alibaba Group.
DingTalk.exe	< 0.01	15,192 K	29,692 K	7604 钉钉	Alibaba Group.
DingTalk.exe	0.37	75,760 K	85,348 K	980 钉钉	Alibaba Group.
DingTalk.exe	< 0.01	52,500 K	52,964 K	7020 钉钉	Alibaba Group.
DingTalk.exe	< 0.01	137,476 K	64,668 K	8020 钉钉	Alibaba Group.
DingTalk.exe		38,716 K	59,360 K	9500 钉钉	Alibaba Group.
DingTalk.exe	25.89	178,164 K	126,856 K	6232 钉钉	Alibaba Group.
calc.exe	1.87	3,368 K	13,128 K	5192 Windows Calculator	Microsoft Corporation

3.2 风险等级

奇安信 CERT 风险评级为：高危

风险等级：蓝色（一般事件）

第4章 影响范围

已知钉钉电脑版<=6.3.5

第5章 处置建议

请尽快升级至安全版本（钉钉电脑版 >= 6.3.25）：

检查钉钉版本(左上角名字->关于钉钉)是否 >= 6.3.25，并打开自动更新（默认打开）

第6章 参考资料

[1] https://page.dingtalk.com/wow/z/dingtalk/default/dddownload-index

奇安信 CERT

【我们是谁】

奇安信应急响应部（又称：奇安信 CERT，奇安信 A-TEAM）成立于 2016 年，是属于奇安信旗下的网络安全应急响应平台，平台旨在第一时间为客户提供漏洞或网络安全事件安全风险通告、响应处置建议、相关技术和奇安信相关产品的解决方案。

奇安信 A-TEAM：团队主要致力于 Web 渗透、APT 攻防、对抗，前瞻性攻防工具预研。从底层原理、协议层面进行严肃、有深度的技术研究，深入还原攻与防的技术本质，曾多次率先披露 Windows 域、Exchange、WebLogic、Exim 等重大安全漏洞，第一时间发布相关漏洞风险通告及可行的处置措施并获得官方致谢。欢迎有意者加入！

【我们的服务】

安全风险通告：奇安信 CERT 成立至今已发布上百篇安全风险通告，从成立至今，针对多个高危漏洞、网络安全事件发布风险通告并给出了有效的安全措施。我们的安全研究团队将实时跟踪安全热点事件和漏洞，始终站在用户的视角去评估风险，致力于第一时间向客户发送有效的风险和相关解决方案。

【订阅方式】

发送接收邮箱和所属单位至：

cert@qianxin.com

【微信公众号】

奇安信 CERT