安全漏洞通告

CVE-2021-32761: 32 位 Redis 远程代码执行漏洞

360CERT
北京奇虎科技有限公司

报告信息

报告名称	CVE-2021-32761: 32 位 Redis 远程代码执行漏洞		
报告类型	安全漏洞通告	报告编号	B6-2021-072201
报告版本	1	报告日期	2021-07-22
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-07-22	360CERT	360CERT	撰写报告

目录

1 漏洞简述

2021 年 07 月 22 日，360CERT 监测发现 Redis官方 发布了 Redis远程代码执行漏洞的风险通告，漏洞编号为 CVE-2021-32761 ，漏洞等级：高危，漏洞评分：8.5。

Redis 是世界范围内应用最广泛的内存型高速键值对数据库。Redis 中存在一处整形溢出漏洞，并可能导致内存越界读。Redis *BIT* 命令与proto-max-bulk-len配置参数结合的情况下能够造成整形溢出，最终导致远程代码执行。

对此，360CERT 建议广大用户及时将 Redis 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。

2 风险等级

360CERT 对该漏洞的评定结果如下

评定方式	等级
威胁等级	高危
影响面	广泛
攻击者价值	高
利用难度	高
360CERT 评分	8.5

3 漏洞详情

3.1 CVE-2021-32761: Redis 整形溢出漏洞

CVE: CVE-2021-32761

组件: Redis

漏洞类型: 整形溢出

影响: 代码执行；服务器接管

简述: 攻击者通过*BIT* 命令与proto-max-bulk-len配置参数结合的情况下，可攻击运行在 32 位的系统中的 32 位的 Redis 程序，该漏洞能够造成整形溢出，并最终导致远程代码执行。

4 影响版本

组件	影响版本	安全版本
Redis:Redis	>2.2/<5.0.13	5.0.13
Redis:Redis	>2.2/<6.0.15	6.0.15
Redis:Redis	>2.2/<6.2.5	6.2.5

5 修复建议

5.1 通用修补建议

根据影响版本中的信息，排查并升级到安全版本

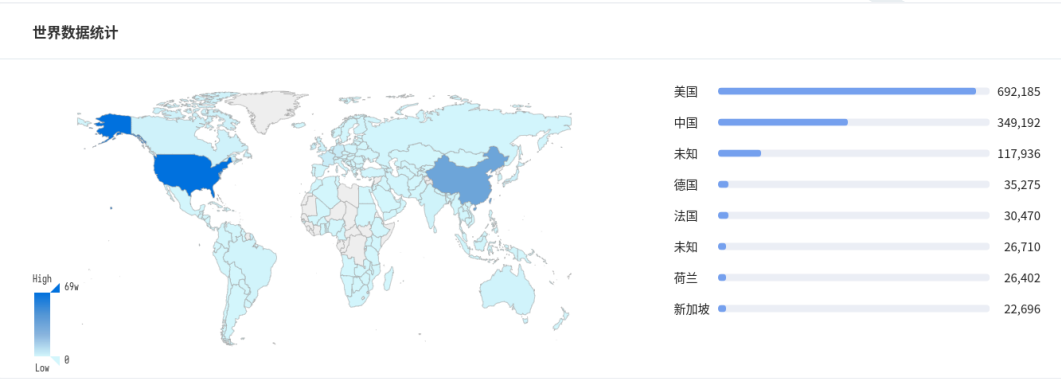
5.2 临时修补建议

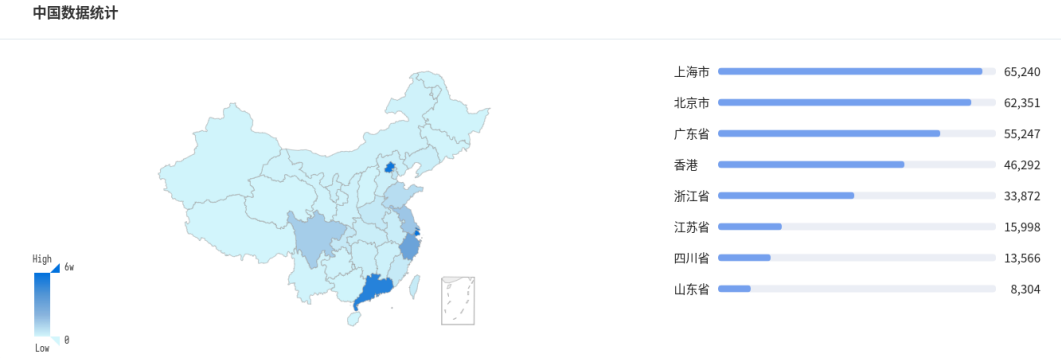
- 禁止低权限用户使用 CONFIGSET 指令
- 替换为 64 位的 Redis 程序

6 相关空间测绘数据

360 安全大脑-Quake 网络空间测绘系统通过对全网资产测绘，发现 Redis 具体分布如下图所示。

Quake 搜索语法：app:"Redis"





7 时间线

2021-07-22 Redis 发布通告以及修复版本

2021-07-22 360CERT 发布通告

8 参考链接

redis/releases

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

A.1 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台 (quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或 (quake#360.cn) 获取对应产品。

A.2 360 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。

A.3 360 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。