2016 中国互联网安全大会
China Internet Security Conference

协同联动 共建安全+命运共同体

安全，不应有旁观者

暨360路由器挑战赛颁奖典礼

时间轴

挑战时间：7月4日-8月5日

1

挑战人员：
打擂方 VS 守擂方
赛事报名选手 VS 360信息安全部

2

挑战规则：
挑战时间内对360 P1路由器从硬件、ROM、APP、网络处理、前端接口、后台接口进行黑客攻击

3

挑战过程：
如选手线下挑战时间发现的漏洞在最终挑战版本仍然可用，可在360安全应急响应中心平台提交漏洞细节

4

挑战版本：
8月6日360P1路由器会公开更新版本，作为攻防双方最终挑战版本。

5

挑战裁定：
提交漏洞细节(可采用技术图文、录像描述的方式)，提交截止时间为8月10日，由评委会确认挑战是否完成

6

7

挑战颁奖：
经评委会评估确认如选手挑战成功，将邀请选手到Hackpwn进行现场颁奖，如未有选手挑战成功，Hackpwn将宣布守擂方获胜。

攻擂方

ISC 2016 中国互联网安全大会

HACK PWN 安全极客狂欢节

邀请 向10支安全团队发出挑战邀请函

申请 1个月以来我们收到了170条申请
活动进行时，日最高申请数达到了41条

审核 共有77人(个人及团队)通过申请审核

守擂方

Unicorn Team

无线电硬件安全团队

Cloud Security Team

云安全团队

Vulpecker Team

Android安全团队

0KEE Team

WEB攻防团队

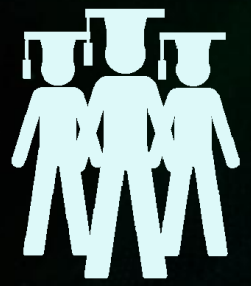
Nirvan Team

iOS安全团队

挑战赛战果

攻方

- 发现提交6个漏洞
- 路由器DNS存在bind漏洞、某CGI未授权访问
- 路由器管理界面jquery版本过低
- 路由器slowhttp拒绝拒绝服务
- 安卓客户端组件配置

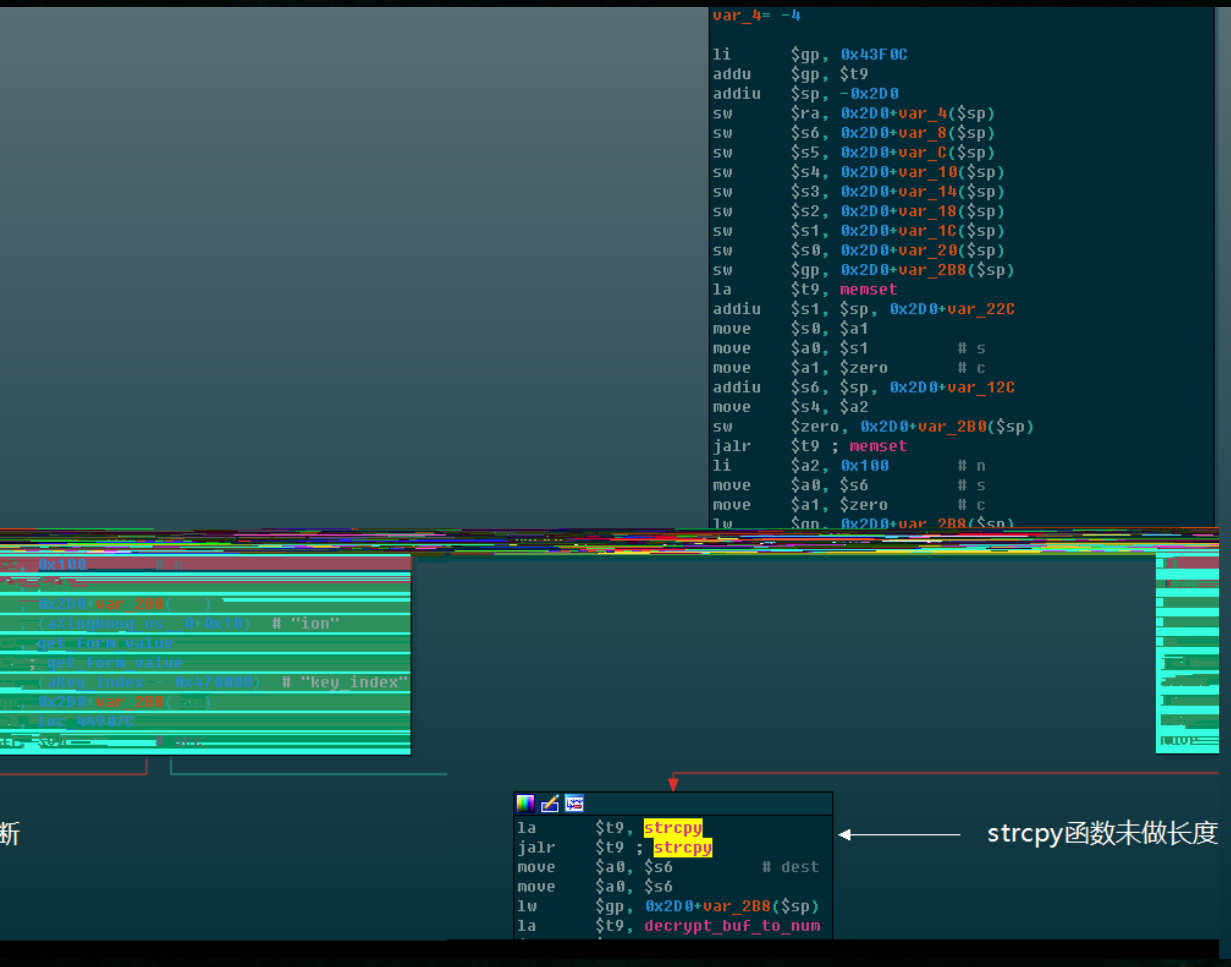


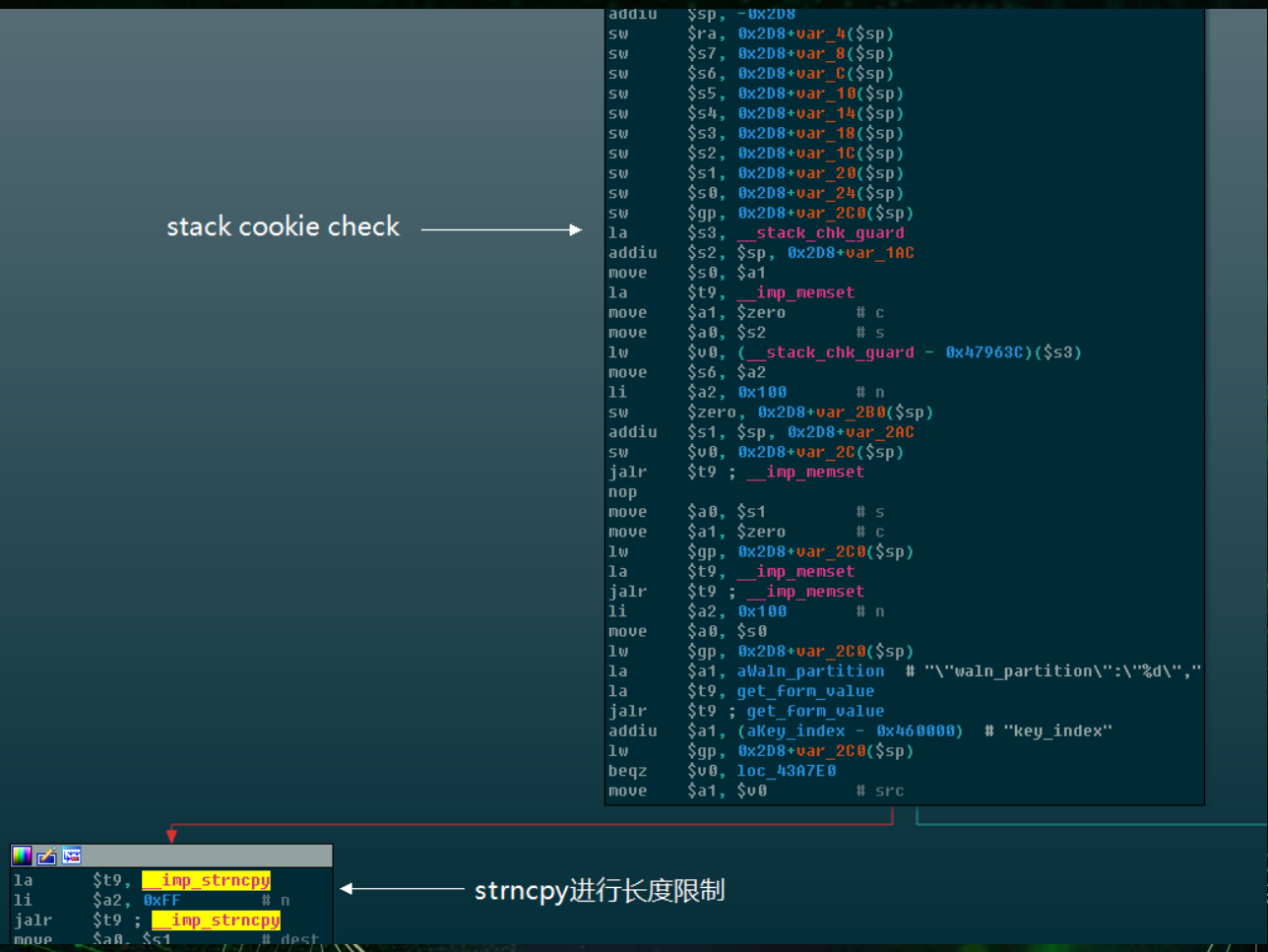
守方

- 发现漏洞42个（不包括不可抗拒漏洞）
- 高危漏洞17个
- 主要包括远程命令执行、缓冲区溢出漏洞、部分第三方插件引入的命令执行问题

对高危漏洞的容忍度只有24小时

某函数对传入的key_index值未做长度判断，使用strcpy直接拷贝到0x100大小的栈内存中，导致缓冲区溢出。

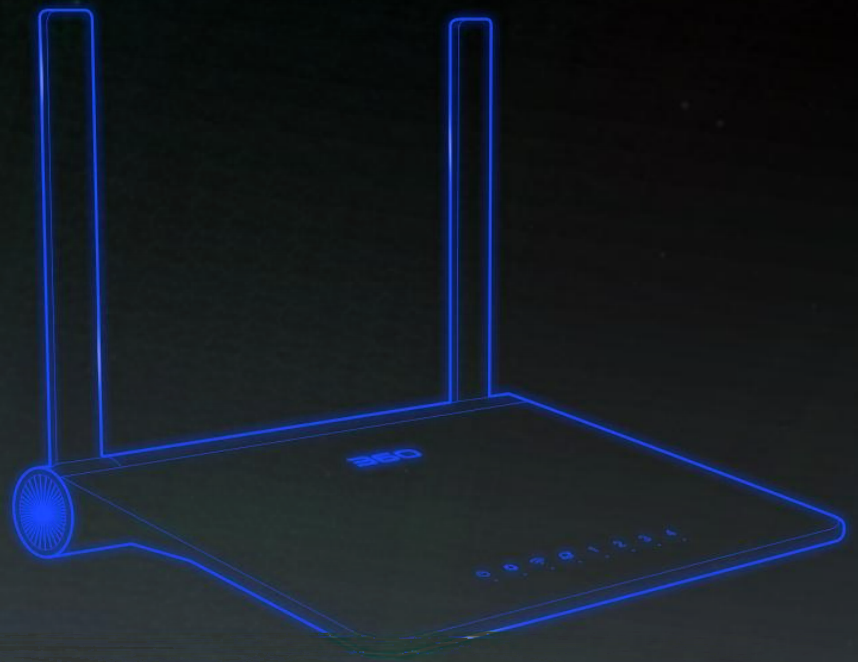




ISC 2016 中国互联网安全大会

HACK PWN 安全极客狂欢节

挑战无止境



《协同共建物联网安全倡议书》

没有绝对安全的系统，只有对安全负责任的态度

伴随着者万物互联时代的来临，网络安全的威胁已经超越信息安全本身，直接关系到人们的财产、人身安全甚至国家基础设施和社会服务的安全。作为网络安全工作者，我们深感责任重大。

万物互联时代，每个连接到网络中的装置都可成为接入网络的路径或入口，也有可能变成恶意者的攻击面，安全也因此面临了前所未有的挑战。任何一家企业和机构都无力确保设备和系统安全或者独立承担安全防御任务。

没有绝对安全的系统，只有对安全负责任的态度，作为网络安全的维护者，我们向全社会发起倡议，呼吁智能设备生产厂商、互联网服务提供商、云服务提供商、网络安全厂商、安全研究机构和全社会的安全极客，积极参与到万物互联网安全防护中，发挥各自优势，协同联动，共同维护IOT时代的安全。

IOT时代的安全，不应有旁观者。

安全，不应有旁观者

ISC 2016 中国互联网安全大会

HACK PWN 安全极客狂欢节

谢谢

中国互联网安全大会

安全极客狂欢节