京麒 网络安全大会

2023 IOTCON

IoT设备漏洞攻防介绍

Alex
京东安全獬豸实验室
安全研究员

关于我们

- 京东安全獬豸实验室 (Dawn Security Lab) 是京东安全旗下重点关注IoT安全、系统安全、核心软件安全、移动安全等前沿基础技术研究的团队。

- 实验室成员曾多次获得Pwn2Own冠军，2022 Pwnie Award最佳提权奖，多次在BlackHat、DEFCON、MOSEC、CanSecWest等会议上演讲，Google Android名人堂排名全球Top30，国内第二；三星安全名人堂国内第一。

- 实验室多次获得Google、Samsung、Apple等的50+公开致谢致谢，并向CNNVD/CNVD等报送多个漏洞。

- https://dawnslab.jd.com

议程

- IoT设备攻击面介绍
- 二进制程序自动化分析实践
- IoT设备漏洞实战

京麒 网络安全大会

IoT设备攻击面分析

选择合适的对象

- 网络设备
  - 路由器、交换机
  - VPN网关
  - 企业边界防火墙、堡垒机
- 办公设备
  - 打印机
  - NAS
  - 摄像头
- 工控设备
  - 无人车
  - 仓储机器人

IoT vs 现代操作系统、软件?

- 产品迭代升级慢
- 软件防御机制不完善
- 历史遗留问题多

更适合CTF Player入门!

IoT设备攻击面分析

常见的攻击入口

Web服务

UPNP

NetTalk

SMB

FTP

SLPD

常见的二进制程序漏洞模式

内存型漏洞	逻辑型漏洞
Buffer越界 • strcpy • base64_decode • strcat	命令注入 • system • popen
整数溢出 • atoi • stroul	路径穿越 • ../ • %2F%2F/
格式化字符串 • sprintf • syslog • sscanf	AUL • 检查认证逻辑 • 检查是否存在越权API调用
memcpy	SQL注入


京麒
网络安全大会
2023
CTFCON
如何高效挖掘品相好的漏洞?

二进制程序自动化分析实践

二进制程序自动化分析

优点

- 节省人力

缺点

- 路径爆炸
- 容易误报

二进制程序自动化分析实践

使用Binary Ninja进行漏洞模式匹配

```python
def check_sprintf(bv, symbol = "sprintf"):
    addr = get_function_addr (bv, symbol)
    if addr == None:
        return []
    refs = bv.get_code_refs(addr)
    ret = []
    for ref in refs:
        func = ref. function
        fmt = func.get_parameter_at(ref.address , None, 1)
        if not is_constant(fmt):
            ret.append((symbol, func.name, ref.address, Error.FORMAT_UNCONSTANT))
            continue
        asc = bv.get_ascii_string_at(fmt. value, min_length = 2)
        if asc == None:
            continue
        fmt_value = asc.value
        cidx = 0
        arg_idx = 1
        while True:
            idx = fmt_value.find("%" ,cidx)
            if idx < 0:
                break
            arg_idx += 1
            cidx = idx + 1
        if fmt_value[idx:].startswith("%s"):
            arg = func.get_parameter_at(ref.address, None ,arg_idx)
            if not is_constant (arg):
                ret.append((symbol, func.name, ref.address, Error.FORMAT_OVERFLOW))
    return ret

```

审计sprintf

1. 获取危险函数的地址（2）
2. 遍历所有的引用（7）
3. 依次检查引用的参数是否安全（9-28）

二进制程序自动化分析实践

优先扫描对外提供服务的程序

- 存在bind、SSL_accept等函数

根据经验增加一些额外的约束：

- strcpy、strcat

  dst参数为栈空间

- system

  同时调用snprintf或sprintf

- sscanf

  调用sscanf的同时没有调用fopen

…

二进制程序自动化分析实践

扫描某款NVR设备固件，在一个udp服务上发现一处命令注入

```
sprintf         function: sysSetDeviceName      addr: 0xca18 Error.FORMAT_UNCONSTANT
strcpy          function: firmware_upgrade      addr: 0xd43c Error.STACKOVERFLOW
strcpy          function: firmware_upgrade      addr: 0xd464 Error.STACKOVERFLOW
strcpy          function: check_passwd          addr: 0xe2ac Error.STACKOVERFLOW
strcpy          function: check_passwd          addr: 0xe2c8 Error.STACKOVERFLOW
system          function: firmware_upgrade      addr: 0xd50c Error.COMMANDINJECT
system          function: firmware_upgrade      addr: 0xd5d0 Error.COMMANDINJECT
system          function: firmware_upgrade      addr: 0xd674 Error.COMMANDINJECT
system          function: firmware_upgrade      addr: 0xd6d4 Error.COMMANDINJECT
system          function: firmware
system          function: firmware
```

```
45    if ( *((_WORD *)v13 + 2) == 0x101 )
46    {
47      system("config_set -x;");
48      if ( chdir("/tmp/xtmp") )
49        goto LABEL_15;
50      *((_DWORD *)a1 + 2) = reply_upgrade_process_buffer(a1);
51      send_buffer_by_interface(a1);
52      memset(v6, 0, sizeof(v6));
53      snprintf(v6, 0x100u, "config_set -b;");
54      system(v6);
55      rename("backup.tgz", s);
56      memset(v6, 0, sizeof(v6));
57      snprintf(v6, 0x100u, "tftp -p -l \"%s\" %s", s, (const char *)ip_addr);
58      system(v6);
59      *((_DWORD *)a1 + 2) = reply_upgrade_done_buffer(a1);
60      send_buffer_by_interface(a1);
61    }
62    if ( *((_WORD *)v13 + 2) != 258 )

000056D4 firmware_upgrade:58 (D6D4)
```


京麒
网络安全大会
2023
IoTCON
IoT设备漏洞实战

京麒 网络安全大会

IoT设备漏洞实战

如何针对特定目标进行二进制漏洞挖掘利用?

信息收集	固件提取	社会工程	设备后门	
	历史漏洞	黑盒测试	攻击面分析	
漏洞挖掘	代码审计	自动化扫描	模糊测试	
漏洞利用	QEMU模拟	NVRAM模拟	用户态模拟	
	Exploit编写	小版本适配	漏洞持久化	后渗透


京麒
网络安全大会
2023
CTFCON
THANKS