陈平

红日学院

工控安全的一千零一种姿势

红日安全 陈平

个人简介

个人介绍

- ID 陈平 / Murkfox
- 男 / 单身
- lsc-sec 安全实验室负责人
- 红日安全核心成员
- 曾多次在国内会议上发表演讲
- 曾在各大论坛发表多篇优秀原创技术文章

目录

工控安全研究方向概述

工控安全是近几年才火起来的研究方向，但工控安全的形势自始至终都是严峻的。

工控安全的研究方向大概分三种

协议分析（分析工控私有协议，挖掘通信过程中的安全问题）

固件分析（分析工控设备固件系统安全，挖掘设备系统中的安全问题）

应用分析（分析具体的工控设备应用程序，包括各种语言的代码审计、二进制逆向、VxWorks固件逆向等）

各类工控设备简介

由于篇幅限制，咱们转移战场

固件逆向分析概述

工控设备固件获取方式

官网下载中心

ABB Schneider

通过组态软件、工控程序设计软件，更新固件处，截取

Schneider 后门账户案例

怼设备，通常值得分析固件的设备都会有 USB ，实在没有的就撬芯片

固件逆向分析概述

常备工具

binwalk : Analyz the firmware

Ghrida : Reverse Vxworks

ubi_reader : Extract extract UBIFS file systems

yaffshiv : Extract YAFFS file systems

jefferson : Extract JFFS2 file systems

Ida_Pro : Reverse ELF and other

Jd-gui : Reverse Java file

LuacGUI : Reverse Luac file

固件逆向分析概述

固件分析思路

1. 解压固件，获取文件系统
2. 查看系统中相关组件及服务配置（/etc| /usr/bin| /usr/sbin ）
3. 逆向分析相关组件，查看是否存在版本漏洞
4. 查找固件应用（Web）文件所在
5. 分析固件应用默认配置安全问题

5.5 对固件应用进行反编译或解密

6. 逆向分析固件应用安全问题
7. 若有设备可结合设备实际运行进行综合安全测试

Thanks