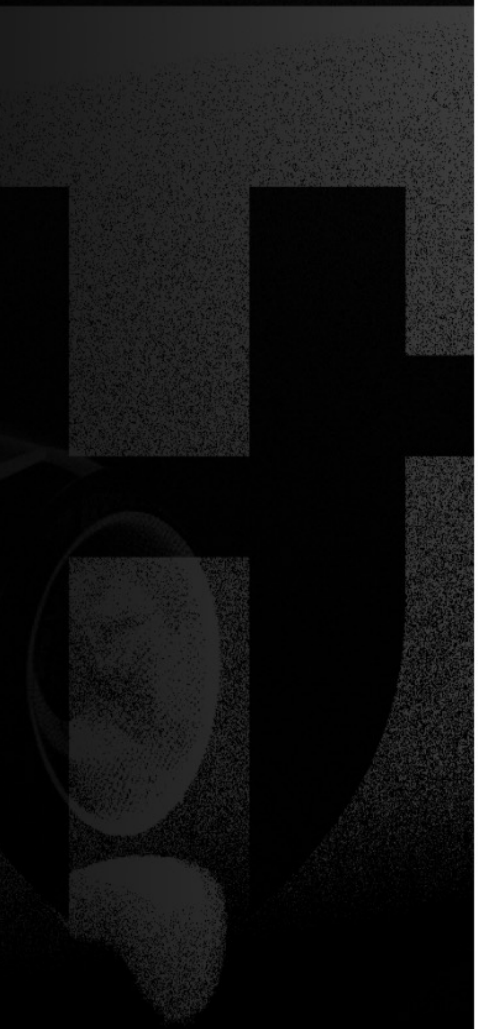
木卫四科技
CALLISTOTECHNOLOGY

2023
智能汽车网络安全威胁报告

前言



2023年智能汽车行业的快速发展引领了技术创新的新浪潮，智能化 为车主带来了丰富的体验，也为网络安全提出了新的挑战。

木卫四汽车威胁情报中心对2023年智能汽车发生的安全事件进行了深入分析，研究了405起安全事件和168个针对汽车的CVE漏洞。在新增事件中涵盖了多种针对汽车资产和远程服务的威胁，例如利用电压故障注入攻击来绕过MCU-Z的AMD安全处理器，攻击特斯拉汽车信息娱乐系统；利用WebSocket通信机制的开放充电站协议（OCPP）漏洞，导致电动汽车充电站无法使用，并导致服务中断；利用T-Box漏洞导致MQTT服务器的地址泄露，攻击者向后端管理车辆的控制器局域网（CAN）注入控制数据等。

虽然攻击方法正在增加，但是我们应该感到庆幸，在木卫四VSOC中所检测到的事件和情报中心分析的全球范围的安全事件及暗网的表现，2023年针对汽车的漏洞和攻击事件大部分源于研究性的破解和攻防比赛、车辆改装以及部分功能安全问题，并通过社区、漏洞应急中心进行了上报，这也为我们应对恶意的汽车网络安全威胁赢得了时间。

随着GPT的兴起，在AI的协助下，诸如对汽车供应链信息的获取，编写攻击脚本，对二进制代码进行逆向分析，ECU固件分析，漏洞挖掘等攻击手段的门槛会进一步降低，攻击方法会呈现多样性；而随着AI在网络安全中的应用，不仅能够帮助我们更有效地识别和消除威胁，还能应对新型攻击手段，提高系统的防护性和可靠性。随着智能汽车系统变得越来越复杂，AI将成为预测和应对未知威胁的关键工具。

智能汽车是否安全不再是单一零部件的问题，而是涉及汽车多种资产和智能化服务的复杂问题，涵盖了针对EEA、软件架构到数据处理，从用户隐私到合规的研究，在这一进程中，将面临新的挑战，同时也迎来新的机遇。

您将从2023年的报告中了解到的细节和洞察包括：

通过对众多组织和安全事件分析，汽车网络安全威胁正持续从单点故障向业务侧迁移；

从汽车域控制器到智能化服务，几个典型的Case Study；

结合ATT&CK的攻击模型框架，受影响的汽车资产和业务，对今年典型安全事件的拆解；

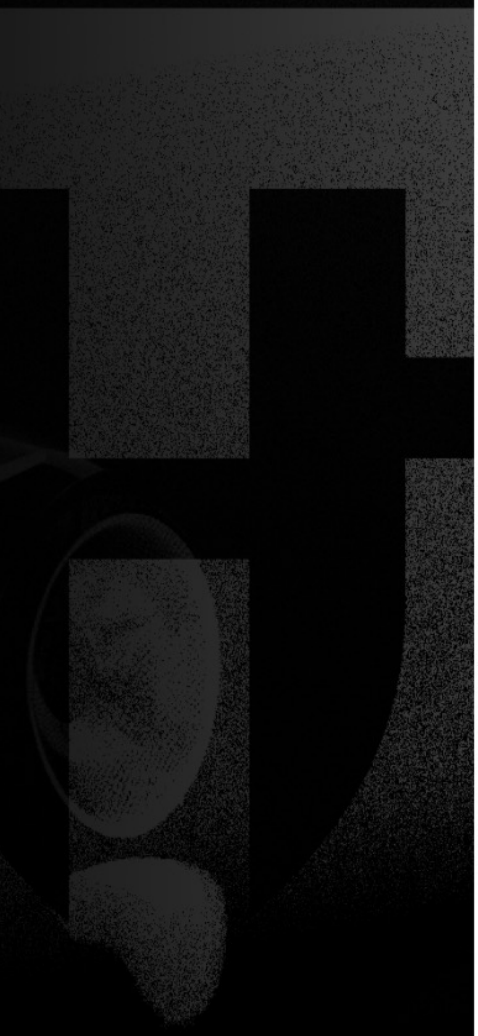
从车企如何更完善的应对汽车网络安全威胁角度出发，创新性提出了汽车安全指数。

这篇对今年汽车安全关键情报信息的综合分析，希望能协助您进一步提升汽车网络安全能力并强化对汽车网络安全态势的感知。

我们将要面对的是软件化带来的汽车工业的高速迭代和全球15亿辆车正在逐步接入到互联网的现状，汽车安全要跟上车厂的技术创新同步发展，而对手正在使用更多样技术试图侵害我们的车辆。随着汽车的每一次创新，可以预想攻击者也会寻找更多的利用方法。

在木卫四，我们遵从通过创新的技术提供高可靠性和易于扩展的汽车网络安全解决方案和服务，从端到云，从机器学习到LLM，随着技术创新到产品的应用，正在实现“为安全出行保驾护航”这一使命。

目录



04 威胁概况
05 全球汽车安全研究机构与组织
06 漏洞及事件的情况
07 持续的威胁
08 2023年典型攻击事件图
09 面对多样攻击的应对方法
10 Case Study-ADAS域控威胁
11 Case Study-PEPS威胁
12 Case Study-充电桩基础设施威胁
13 车企网络安全指数
15 安全建议
17 产品与服务
19 关于我们

40+
跟踪机构与组织

160+
研究汽车安全漏洞

400+
分析汽车安全事件

木卫四在汽车网络安全威胁分析上集合了过往的漏洞、安全社区内容、安全事件、暗网信息等来源，再加入汽车的专属特征进行了针对性分析，旨在帮助您更好的了解2023年全球汽车网络安全状况。

2023年，木卫四汽车威胁情报中心持续监控和分析全球范围内智能汽车网络安全的最新动态。我们紧密跟踪全球40+汽车安全研究机构和组织，专注于分析400多起智能汽车领域的网络安全事件，并深入研究160多个智能汽车系统中存在的安全漏洞。我们研究发现当前面临的威胁涵盖了TSP服务、智能座舱、充电服务、车主APP、TBox以及数据泄露等方面。

在Blackhat 2023会议上，柏林工业大学的三名博士研究生和安全研究员Oleg Drokin展示了破解特斯拉AMD Zen 1安全处理器（ASP）的过程。他们使用电压故障注入技术绕过了安全启动的固件完整性校验，成功提取固件并植入后门之后，重新烧录至Flash存储，从而获得车载信息娱乐系统的root权限。他们还研究了TPM对象的密封与解封过程，并从NVMe存储中提取了系统和用户的敏感数据。

SaiFlow研究团队发现OCPP1.6 Websocket存在漏洞，该漏洞可能导致远程操作充电桩拒绝服务或实现免费充电。漏洞的具体影响取决于充电桩的本地配置，例如是否支持离线身份认证以及是否允许对未知车辆提供充电。研究表明，攻击者可利用URL中的充电桩ID（如CP3211）发起连接请求，影响正常会话。

Medusa勒索软件组织在其暗网数据泄漏站点上将丰田金融服务列为受害者，要求支付800万美元的赎金以防数据泄露，并给予丰田10天的回应期限，逾期每日加收1万美元滞纳金。作为攻击证据，Medusa公开了财务文件、电子表格、采购发票、账户密码、护照扫描等敏感信息。

GitHub用户zj3t开发了一个针对大众汽车信息娱乐系统的媒体文件模糊测试工具。通过测试超过2万个媒体文件，他发现了OGG文件格式的漏洞。这个漏洞在USB自动播放媒体文件时触发，导致信息娱乐系统无法重新启动，只能手动重启以恢复。此漏洞可能存在远程代码执行的安全风险。

全球汽车安全研究机构与组织

经过多年的深入研究，汽车网络安全领域持续揭露新的攻击手段和安全漏洞。在专注于汽车网络安全的机构和个人的不懈努力下，汽车网络安全问题正日益成为公众和行业关注的焦点。

机构种类	机构名称
黑客组织	Agenda
安全公司	Baidu X-team
白帽子	Corben Leo
研究机构	Cybernews Research Team
白帽子	Eaton Zveare
安全公司	EDAG Group
安全公司	Emsisoft
黑客组织	Medusa
白帽子	Oleg Drokin
安全公司	Saiflow
安全公司	Synacktiv
研究机构	Technical University of Berlin
安全公司	Xiaomi Smart Terminal Security Lab
研究机构	Yuga Labs

注：依据对汽车安全研究活跃度选择部分机构与组织，机构名称依据字母顺序排列，排名不分先后。

攻击从单一零部件向业务迁移

2023 VS 2022漏洞数量

34%↓

2023 VS 2022安全事件

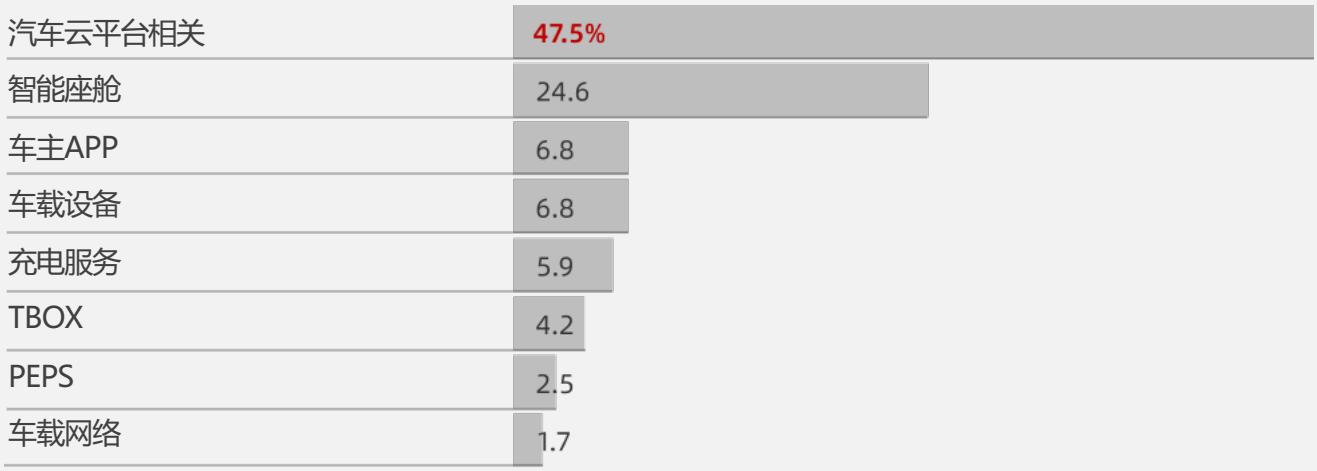
25%↑

核心零部件和智能化服务的威胁

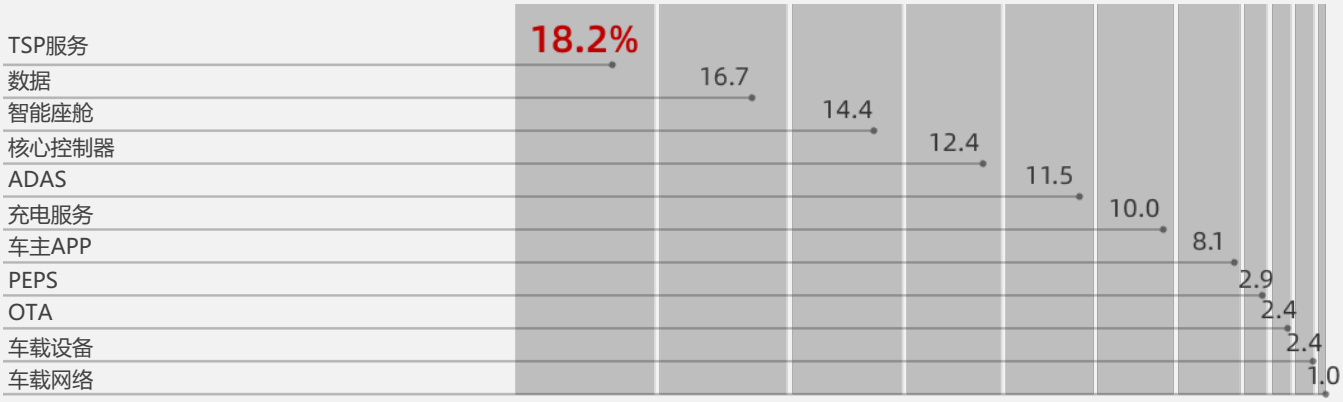
近年来随着智能汽车技术的快速发展，针对智能汽车的攻击也逐渐从传统的针对单一车辆控制器的攻击转变为针对整车智能化服务的攻击，包括但不限于对远程控制应用程序的操控、云服务的渗透、智能座舱系统的破解以及对第三方应用和智能服务的攻击。

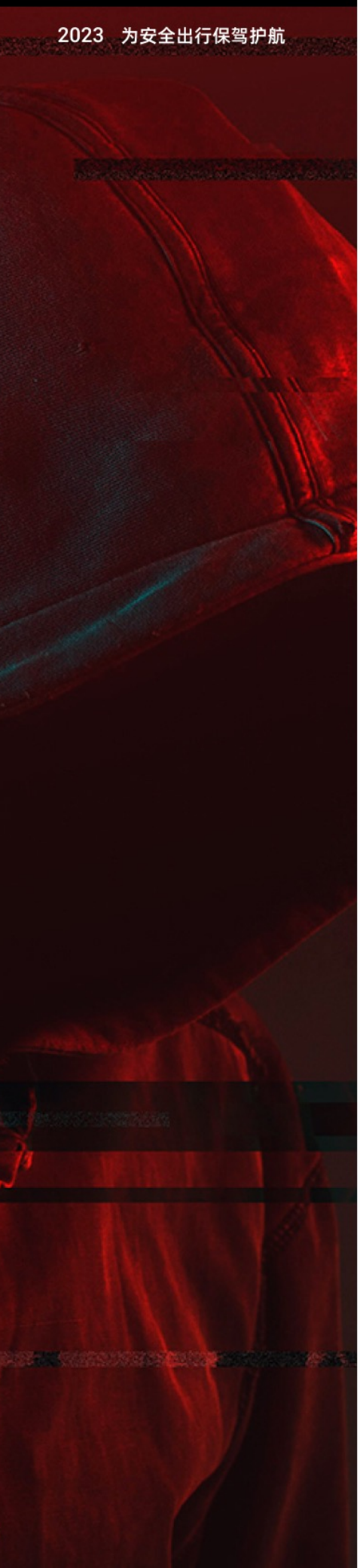
随着WP.29 R155&R156的合规要求，车企已经建立了全面的网络安全管理系统，保证车辆生命周期的安全。尽管如此，依然有越来越多的智能化服务漏洞被曝出，影响智能汽车的安全。

2023年汽车漏洞百分比



2023年汽车安全事件百分比





持续的威胁

TSP服务威胁

木卫四威胁情报中心分析了2023年以来的汽车漏洞，我们发现47.5%的漏洞均与TSP服务有关。在已知的汽车漏洞中，与TSP服务相关的漏洞主要涉及云端配置错误、云端Token泄漏、认证机制绕过、API权限滥用等。攻击者利用这些漏洞可完成对单一车辆的远程控制，甚至能够实现批量控车。

智能座舱威胁

智能座舱在2023年依然成为研究者持续研究的对象，研究者们发现多个与智能座舱相关的漏洞威胁，其中包括绕过车机固件升级的签名机制，在车机系统中植入恶意后门；通过对车机音频解码器进行模糊测试，造成播放器的崩溃；利用蓝牙芯片模组中的堆溢出漏洞和越界写漏洞实现对车机的控制；采用电压故障注入绕过安全启动，获得车机系统的Root权限。

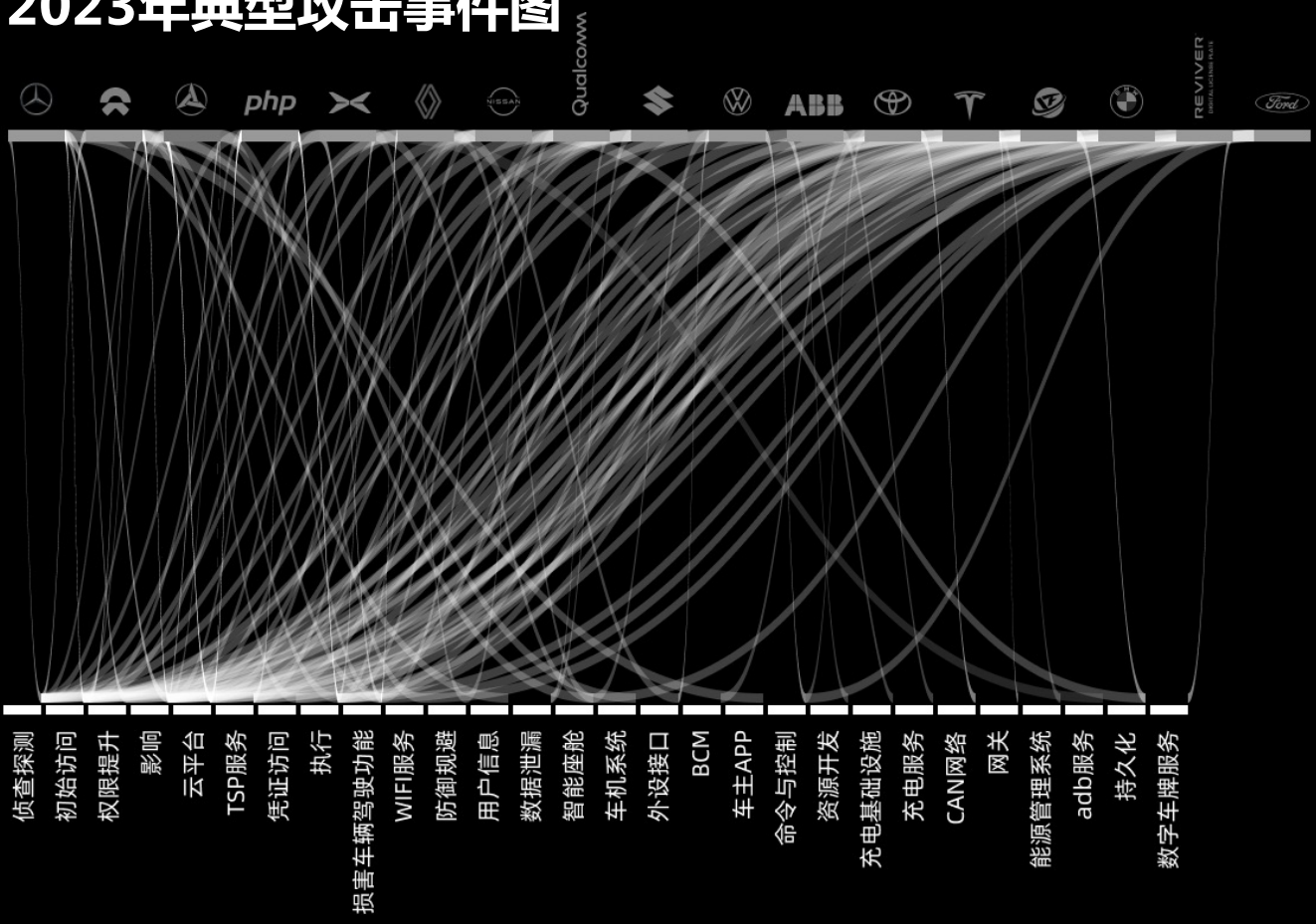
充电服务威胁

随着电动汽车（EV）的普及，充电桩的网络安全显得尤为重要。当前充电服务主要面临以下四种威胁，一是远程干扰漏洞，如“Brokenwire”漏洞，能够远程扰乱大规模的EV充电；二是协议利用攻击，利用开放充电点协议（OCPP）发起的攻击，可能导致充电点遭受拒绝服务攻击；三是未经授权访问，涉及未授权访问充电站系统，可能威胁数据安全；四是远程接管威胁，通过蓝牙低能耗（BLE）技术漏洞实现远程接管充电器。

车主APP威胁

车主APP作为远程控制车辆和实时监测车辆状态的智能化应用，面临的威胁也持续增加，依据2023年追踪的汽车漏洞与安全事件分析，存在的威胁涉及三种，第一种远程控制威胁，攻击者利用API漏洞实现车辆的远程控制，其中包括解锁车门、启动引擎甚至干预车辆行驶；第二种账户安全风险，车主APP账户可能遭受攻击者攻击，攻击者利用盗用的账户实现车辆的控制；第三种是数据隐私泄漏，车主APP收集的数据可能包含敏感信息，如位置数据和行驶习惯 ， 这些数据若被不当访问或滥用，可能导致严重的隐私问题。

2023年典型攻击事件图



奔驰
Mercedes me IOS APP v1.34.0及以下版本中的访问控制问题允许攻击者查看其他用户的维护订单并通过未指定的向量访问敏感的用户信息。

蔚来
蔚来车机存在错误配置和目录遍历漏洞,可提权至Root。

三一重工
ASRG-China 社区发现三一重工等企业T-Box超危漏洞。

phpscriptpoint
phpscriptpoint Car Listing 1.6（汽车列表目录内容管理系统（CMS））存在漏洞（CVE-2023-3858 和 CVE-2023-3859）。

小鹏
小鹏汽车打开开发者模式，实现APP的任意安装。

雷诺
雷诺 Zoe EV 2021 汽车信息娱乐系统USB漏洞。

日产
日产澳大利亚和新西兰业务遭受网络攻击。

Qualcomm
汽车操作系统平台 Android 中的访问控制不当。

铃木
铃木汽车泄露敏感信息。

大众
大众汽车车机存在漏洞。

ABB
车辆充电平台面临盗刷威胁。

丰田
“车头灯黑客”通过 CAN 干扰窃取汽车。

特斯拉
特斯拉网关遭受TOCTTOU攻击。

延锋
延锋遭“麒麟”勒索软件攻击，致北美工厂生产中断。

宝马
通过错误配置的 SSO 接管 BMW 和 Rolls Royce 的完整帐户。

Reviver
加州新数字车牌遭黑客攻击。

福特
福特称存在 WiFi 漏洞的汽车仍可安全驾驶。

面对多样攻击的应对方法

深入了解业务

汽车安全团队通过安全基线、安全架构设计、VTA验证及安全运营，进一步了解公司不同车型的EEA、软件架构和车辆提供的智能化服务。

提升专业能力

从汽车核心资产和智能化服务入手，高级安全研究人员需要尽快从传统的IT攻防手段迁移到针对汽车网络安全的技术研究上来。

引入针对性的威胁监控平台

加快汽车接入专门的安全监控和运营平台（VSOC），利用云计算和AI的能力，在大面积威胁一旦产生时，可以迅速缓解危害，这一举措能大大降低威胁所造成的品牌风险。

加入社区

安排专人加入汽车网络安全社区可以提升企业对风险的感知能力。

Case Study - ADAS域控威胁

随着辅助驾驶功能的丰富，ADAS域控不可避免地暴露出了多个潜在攻击面。攻击方法包括：低功耗CAN总线的短时注入攻击、传感器信号的误导攻击、后台管理接口的破坏性代码注入，以及直接通过控制指令篡改车辆行为。更严重的是，这些攻击很可能利用汽车的功能安全，影响车辆行车安全。

初始访问

攻击者使用nmap扫描到域控某子设备开启了22端口，采用暴力破解的方式获得了正确的登录口令。

命令执行

攻击者通过调试口登录到该域控子设备，通过ps –A命令查看其运行的进程，通过进程名猜测其主要功能，使用scp命令上传敏感文件。

持久化命令执行

攻击者通过调试口传输由telnet指令构造的反向连接脚本，开启反向连接后，获得远程执行权限。

横向移动

攻击者在域控制器中上传nmap工具，并使用此工具探测网络，发现两个IP开放端口22，通过BrutesPray暴力破解登录口令，最终利用22端口登录到内网其中一个IP子网设备中。

功能破坏

攻击者通过kill命令杀死自主泊车服务进程，使此自主泊车功能失效，系统重启。

横向移动

攻击者利用22端口登录到内网中另一个IP子网设备中。

功能破坏

攻击者获取域控制器root权限后，可能定位并终止原有定位服务进程，替换为恶意程序，致使车辆RTK高精度定位服务失效，影响导航与行车安全。

Case Study - PEPS威胁

木卫四汽车威胁情报中心发现2023年针对智能汽车PEPS攻击手段主要包括BLE中继攻击、 RF重放攻击、 CAN注入以及防盗技术绕过。尤其是NCC去年提出的在蓝牙链路层进行中继的攻击方法，对目前市面上大多数蓝牙汽车钥匙有效。

BLE链路层中继

木卫四汽车威胁情报中心监测到有盗贼采用蓝牙链路层中继设备完成偷车行为。中继设备转发链路层PDU，控制连接事件间隔实现了中继操作。该攻击的狡猾之处在于受害者IOS或安卓应用层无察觉，即使蓝牙链路层加密也无法抵抗该攻击。

RF重放&无防盗技术

根据情报中心数据显示，近几年发生射频信号中间人攻击的事件屡见不鲜，直至今日旧的车型仍有概率存在无防盗和RF钥匙重放攻击的问题。

CAN注入

通过追踪暗网发现了一种物理盗窃手段，攻击者通过拆卸大灯接入暗网上高价购买的紧急启动设备，发送CAN报文解锁车辆。被盗车辆数字钥匙ECU和车灯ECU在同一CAN局域网，由于CAN总线广播的特性，车辆执行了禁用防盗和打开车门的指令。

防盗绕过

2023年，美国仍有大量现代汽车和起亚汽车没有使用防盗技术，盗窃者只需用usb插入点火装置即可启动引擎，现代汽车集团因此召回近400万辆车。木卫四汽车威胁情报中心提醒业界目前国内外强标要求车企保障车辆的全生命周期的安全，车企应广泛应用OTA技术和VSOC安全运营来保障对已售车辆的持续更新和维护。

影响

木卫四汽车威胁情报中心预测中继攻击将继续成为汽车盗贼的主要作案手段，原因有三点，一是基于目前防盗技术的大范围应用，重放攻击或滚动码攻击只能打开车门无法启动引擎，无法达到盗贼的目的；二是中继设备成本低，如果在暗网流通会产生比较大的收益；三是中继攻击不像校验绕过或硬件漏洞需要专家级别的攻击者才能实现，中继设备使用简单，攻击者容易上手操作。

Case Study

充电基础设施威胁

充电桩引起的拒绝服务和数据泄露

2023年2月，出现在OCPP 1.6 协议中的漏洞引起业内广泛关注，根据 OCPP 协议标准1.6J版本的安全扩展，充电桩向 CSMS 进行身份验证时支持三种身份验证方法，分别是仅充电桩标识、充电桩身份和凭据、充电桩标识和客户端证书。当采取仅充电桩标识认证方式时，可能会导致充电站DOS攻击，攻击者可能利用合法充电桩重新连接CSMS的时间差窃取能源，或者获取合法充电桩敏感信息并进一步滥用信息。

攻击者可以结合充电站信息泄露进一步扩大影响范围—黑客可在搜索引擎上检索运营商OCPP终端的安装手册，获取运营商服务URL，或者检索运营商充电服务的网站，通过网站API 暴露的数据，发现充电站相关标识符信息。结合以上信息泄露可使大规模充电站遭受OCPP协议身份验证绕过的问题影响。

研究人员不断致力于充电基础设施的安全研究，从2020年以来，发现了多个充电基础设施问题。典型的安全问题包括施耐德充电桩web后台硬编码漏洞，固件验签算法存在缺陷可刷入恶意固件获取充电桩root权限问题，无感支付充电桩GB/T 27930充电机与电池管理系统之间的协议漏洞造成能源窃取。充电基础设施因涉及多个组织，由于组织之间的通信复杂，容易在通信协议上出现逻辑问题和校验不当的问题。

OEM - VCSI

车企网络安全指数

随着智能网联汽车技术的快速发展，网络安全成为各车企的重要考量。OEM-VCSI(OEM Vehicle Cyber Security Index)旨在评估汽车制造商在网络安全方面复杂且不断演变的状态。

车企、Tier1可以依托VCSI作为一种评估机制，从0-10分的角度，评估其在汽车网络安全上的投入和缺陷

网络安全指数

人员结构

存在着不成熟的团队配置问题，仍然有功能安全兼任网络安全的情况，40%的OEM企业完成了由高级汽车安全专家和汽车工程师组成的复杂人员配置的转型。

投入预算

汽车网络安全预算在总研发预算中的平均比例为2%，远远低于传统网络安全，鉴于网络威胁的增加和智能汽车系统的复杂性，这一点尤为令人关注。

安全基线

汽车公司越来越关注法规合规性和标准，如WP.29和ISO/SAE 21434，这些标准强调了网络安全实践的基础标准。有大约40%的企业开始转变建立汽车网络安全基线。

业务理解

智能汽车网络安全的重要性体现在保护车辆免受外部攻击、维护驾驶员和乘客安全，这需要在汽车EEA的核心资产和智能化服务上有比较深入的理解，当前20%的企业汽车安全团队已经开始深入到业务流程和设计决策中。

运营能力

当前90%车企尚未准备好高效运营网络安全。车辆安全运营中心（VSOC）的引入代表了行业运营能力的发展，它提供了一种更全面、综合网络风险管理方法，但面对百万级车辆的安全应对还待积累沉淀。

创新技术

车企在应对新型网络威胁方面表现出较高的积极性，例如远程控车漏洞和电动车充电基础设施攻击，这需要创新技术来解决这些新型挑战，大约50%的企业在2023年有明确的目标投入和规划趋势。

安全建议

五个措施

01

对核心资产和智能化服务的深入理解

汽车的网络安全策略需要从核心资产和智能化服务的角度出发，进行系统级的资产识别，包括车载网络、控制系统和数据存储的关键组件。同时，应分析智能化服务的数据流和依赖关系，确定潜在的安全风险点，并制定相应的安全策略。

02

持续漏洞评估和供应链威胁情报共享

定期进行系统级的漏洞扫描，涵盖车辆的所有关键组件。同时，与供应商共享安全信息，包括已知漏洞和修补程序，确保整个供应链的安全。参与威胁情报共享平台，以获取和分享最新的安全威胁信息。

03

考虑云服务及策略部署

利用云计算的弹性和安全性优势，将云服务集成到车辆系统中，如利用云服务进行大数据分析和威胁监测。

人工智能在异常检测和自动化响应方面的应用将是未来VSOC的重要发展方向。

04

了解攻击者并进行模拟演练

通过持续的威胁情报和攻击模式分析，了解潜在的攻击者和攻击手段。

定期组织红队攻击模拟和蓝队防御演练，以实战方式检验安全策略的有效性。

05

技能与知识的持续提升

鼓励汽车安全工程师不仅深入了解技术细节，还要理解这些技术如何与业务目标和车辆智能化服务相结合。

探索和学习如人工智能、大语言模型、域控边缘计算等新兴技术在网络安全中的应用。

产品和服务

VSOC 汽车网络安全运营平台

持续监测和响应

对车辆核心资产和智能化服务进行持续监测，对不同时间传感器、ECU指令、MCU操作、网络操作、系统操作、应用和数据进行持续监测，颗粒度可以细化到不同用户不同车辆的操纵行为。

AI发现未知威胁的攻击

利用孪生技术建立车辆的安全模型，对物理世界及数字世界的车辆状态交叉分析，结合机器学习实现未知攻击的异常分析 。

高级自动化分析

依照异常事件模版全面获取并自动化分析多达200项的汽车异常事件，并可以追溯到网络包内容、控车指令、API指令等细粒度级别。

全局可视可控

可自动适配拖拽的全局大屏，自定义不同屏幕的监测信息，涵盖网络安全、系统安全、在线服务、异常状态、供应链信息等数十维度的展示概览。

VTI汽车威胁情报

智能车辆构建的威胁情报及漏洞管理解决方案。产品专注于收集、分析和发布汽车行业的威胁情报，并针对车厂、Tier1、联网汽车服务提供商、车队等提供量身定制的汽车威胁情报服务。

漏洞全生命周期管理机制

支持漏洞监测、漏洞识别、漏洞分析、漏洞修复以及漏洞验证等全生命周期的管理。

多源漏洞情报数据融合

支持公开漏洞、供应链漏洞、公开新闻报道、深网/暗网、汽车论坛、学术研究、汽车白帽子/安全团队、汽车漏洞挖掘等多源威胁情报数据的融合。

漏洞优先级评估技术

支持汽车漏洞优先级的评估，有效分配资源，最大程度地降低潜在的安全风险。

WP.29 R155差距分析

支持合规差距分析，产出合规差距分析报告，为车企及供应商提供定制化报告。

VDR 汽车域控信息安全解决方案

通信和网络安全

支持域控外部连接安全和域内安全通信协议。

操作系统安全

支持系统安全事件检测、安全配置检测以及运行状态异常检测。

异常检测和监控

支持漏洞检测、敏感文件监控以及应用程序检测。

敏感数据安全

提供针对敏感数据和关键日志的加密SDK。

关于我们

木卫四科技
CALLISTOTECHNOLOGY

木卫四由全球首批专注于汽车网络安全的技术专家们创立，得益于在汽车网络安全领域多年的积累，使得我们可以从攻防相长的角度出发，并融合先进的人工智能和知识图谱引擎能力，通过算法分析车联网海量的多源异构消息、指令和API服务，从而抵御针对车企和供应链的新型车联网攻击，为智能网联汽车提供威胁感知和防御能力，保护汽车核心资产和智能服务的安全性。

我们对汽车及网络安全行业保持着巨大的热情和兴趣，同时我们尊重并充分学习汽车产业多年以来的工程经验与行业实践，致力于为企业提供更为专业、领先的安全产品与服务。木卫四强调充分释放数据价值，同时强调科学的分析方法与实际的应用服务相结合，多面刻画车辆安全状态，自动分析异常并处置风险，丰富分析维度，减少安全人员运营压力。

木卫四（北京）科技有限公司

官网：
https://www.callisto-auto.com

联系邮箱：
contact@callisto-auto.com

参考引用

1.https://www.bleepingcomputer.com/news/security/tesla-infotainment-jailbreak-unlocks-paid-features-extracts-secrets/

2.https://www.saiflow.com/blog/hijacking-chargers-identifier-to-cause-dos/

3.https://phishingtackle.com/articles/toyota-tfs-targeted-by-medusa-ransomware-suspected-citrix-bleed-vulnerability/

4.https://github.com/zj3t/Automotive-vulnerabilities/tree/main/VW/jetta2021

5.https://www.dailymail.co.uk/news/article-12790145/350-000-Rolls-Royce-GONE-30-seconds-Moment-key-car-thieves-steal-luxury-SUV-owners-driveway.html

6.https://kentindell.github.io/2023/04/03/can-injection/

7.https://www.bleepingcomputer.com/news/security/hyundai-kia-patch-bug-allowing-car-thefts-with-a-usb-cable/