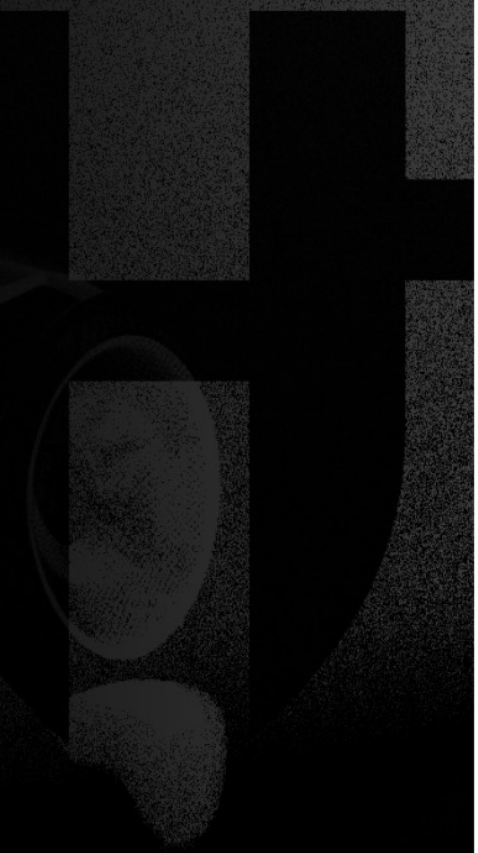
Automotive Cybersecurity Threat Report

2023

CALLISTO

Forward



The rapid development of the smart car industry in 2023 led to a new wave of technological innovation, especially in areas such as intelligent services, autonomous driving functions and smart charging stations. These technological advancements not only greatly improve driver experience, but also pose new challenges to vehicle security.

The Callisto Automotive Threat Intelligence Center conducted an in-depth analysis of security incidents that occurred in smart cars in 2023, studying 405 security incidents and 168 CVE vulnerabilities targeting automobiles. The newly added incidents include a variety of threats against automotive assets and remote services, such as using voltage fault injection attacks to bypass the AMD security processor of MCU-Z, attacking the infotainment system of Tesla cars; exploiting the Open Charge Point Protocol (OCPP) vulnerabilities of WebSocket communication mechanisms, resulting in electric vehicle charging stations becoming unusable and causing service interruptions; and utilizing T-Box vulnerabilities to leak MQTT server addresses, where attackers inject control data into the Controller Area Network (CAN) of the backend management of vehicles.

Although the methods of attack are increasing, we should feel fortunate that among the incidents detected in the Calisto VSOC and the analysis of global security events and the dark web performance by the Intelligence Center, the majority of the vulnerabilities and attack incidents against vehicles in 2023 mostly originated from research-based hacking, defense competitions, vehicle modifications, and some functional safety issues. These were reported through the community and the Vulnerability Emergency Response Center, which also won us time to deal with malicious automotive cybersecurity threats.

With the rise of GPT, the threshold for attack methods such as obtaining information on the automotive supply chain, writing attack scripts, reverse-engineering binary code, analyzing ECU firmware, and vulnerability mining will be further reduced with the help of AI, leading to a diversification of attack methods. Meanwhile, as AI is applied in cybersecurity, it can not only help us identify and mitigate threats more effectively but also deal with new types of attack methods, enhancing the defense and reliability of systems. As intelligent vehicle systems become increasingly complex, AI will become a key tool for predicting and responding to unknown threats.

The safety of smart cars is no longer an issue of a single component, but a complex issue involving multiple automotive assets and intelligent services. This includes considerations from the Electrical/Electronic Architecture (EEA), software architecture to data processing, and from user privacy to compliance research. In this process, new challenges will be faced, as well as new opportunities will arise.

The details and insights you will learn from the 2023 report include:

Through the analysis of numerous organizations and security events, automotive cybersecurity threats are continuously shifting from single-point failures to the business side;

From vehicle domain controllers to intelligent services, several typical Case Studies;

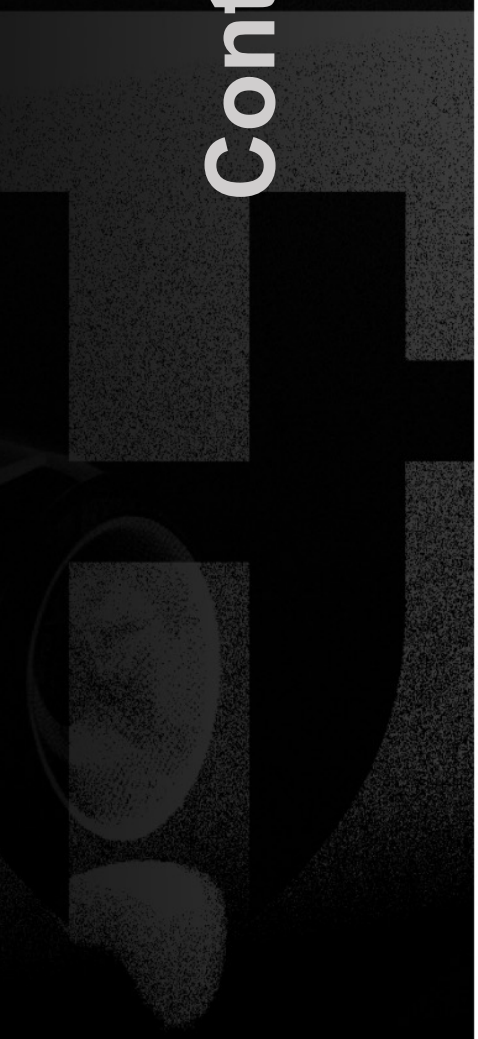
Combining the ATT&CK attack model framework, the affected automotive assets and services, and the dissection of this year's typical security incidents;

From the perspective of how car companies can more effectively respond to automotive cybersecurity threats, an innovative automotive safety index has been proposed.

This comprehensive analysis of this year's critical automotive security intelligence information hopes to assist you in further enhancing your automotive cybersecurity capabilities and strengthening the perception of the automotive cybersecurity situation. What we are facing is the rapid iteration of the automobile industry brought about by software and the current situation where the world’s 1.5 billion vehicles are gradually being connected to the internet. Automotive safety needs to develop in sync with the technological innovations of car manufacturers, while our adversaries are using a more diverse range of technologies and attempting to breach our vehicles. With each innovation in automobiles, it can be anticipated that attackers will also find more methods to exploit.

At Callisto, we adhere to providing highly reliable and easily scalable automotive cybersecurity solutions and services through innovative technology, from end to end, from machine learning to LLM. With the application of technological innovations to products, we are realizing the mission of 'ensuring safe travel'.

Content



40+

Institutions and Organizations Tracked

160+

Automotive Security Vulnerabilities Researched

400+

Automotive Security Incidents Analyzed

Callisto has assembled a collection of past vulnerabilities, security community content, security incidents, and dark web information for automotive cybersecurity threat analysis. By incorporating the unique characteristics of automobiles, targeted analysis has been conducted with the goal of helping you better understand the global automotive cybersecurity situation in 2023.

"In 2023, the Callisto Automotive Threat Intelligence Center continues to monitor and analyze the latest developments in global smart car cybersecurity. We closely follow over 40+ automotive security research institutions and organizations worldwide, focusing on the analysis of more than 400 cybersecurity incidents in the field of smart cars and the in-depth study of over 160 security vulnerabilities in smart car systems. Our research finds that the current threats cover TSP services, smart cockpits, charging services, car owner apps, T-Box, and data leakage, among others.

At the Blackhat 2023 conference, three doctoral students and security researcher Oleg Drokin from the Technical University of Berlin demonstrated the process of cracking Tesla's AMD Zen 1 Security Processor (ASP). They used voltage fault injection techniques to bypass the secure boot's firmware integrity check, successfully extracted the firmware and implanted a backdoor, then re-flashed it to the Flash storage, thus obtaining root permissions of the in-car infotainment system. They also studied the sealing and unsealing process of TPM objects and extracted sensitive system and user data from NVMe storage.

The SaiFlow research team discovered a vulnerability in OCPP1.6 WebSocket that could lead to remote operation of charging piles denying service or achieving free charging. The specific impact of the vulnerability depends on the local configuration of the charging pile, such as whether it supports offline identity authentication and whether it allows charging for unknown vehicles. The study shows that attackers can initiate a connection request using the charging pile ID in the URL (such as CP3211), affecting normal sessions.

The Medusa ransomware organization listed Toyota Financial Services as a victim on its dark web data leak site, demanding an $8 million ransom to prevent data leakage and giving Toyota a 10-day response period, with a daily late fee of $10,000 if overdue. As proof of the attack, Medusa published sensitive information such as financial documents, spreadsheets, purchase invoices, account passwords, passport scans, etc.

GitHub user zj3t developed a media file fuzz testing tool for Volkswagen's infotainment system. By testing over 20,000 media files, he discovered a vulnerability in the OGG file format. This vulnerability is triggered when USB media files are played automatically, causing the infotainment system to be unable to restart, and can only be manually rebooted to recover. This vulnerability may pose a risk of remote code execution."

Global Automotive Cybersecurity Research Institutions and Organizations

After years of in-depth research, the field of automotive cybersecurity continues to reveal new attack methods and security vulnerabilities. Thanks to the relentless efforts of institutions and individuals focused on automotive cybersecurity, the issue of automotive cybersecurity is increasingly becoming a focal point of public and industry attention.

	Institution Type	Institution name
	Hacker Organization	Agenda
	Cybersecurity Company	Baidu X-team
	White Hat	Corben Leo
	Research Institution	Cybernews Research Team
	What Hat	Eaton Zveare
	Cybersecurity Company	EDAG Group
	Cybersecurity Company	Emsisoft
	Hacker Organization	Medusa
	White Hat	Oleg Drokin
	Cybersecurity Company	Saiflow
	Cybersecurity Company	Synacktiv
	Research Institution	Technical University of Berlin
	Cybersecurity Company	Xiaomi Smart Terminal Security Lab
	Research Institution	Yuga Labs

Note: Institution names are arranged in alphabetical order.

Attacks from single components to intelligent services

2023 vs 2022 Number of Vulnerabilities

34% ↓

2023 vs 2022 Security Incidents

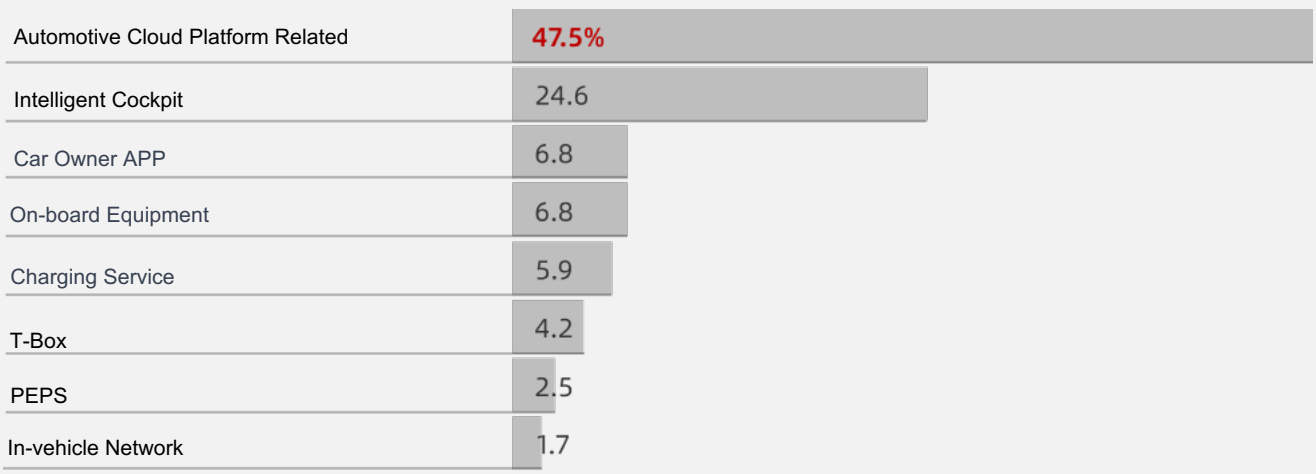
25% ↑

Threats to core components and intelligent services

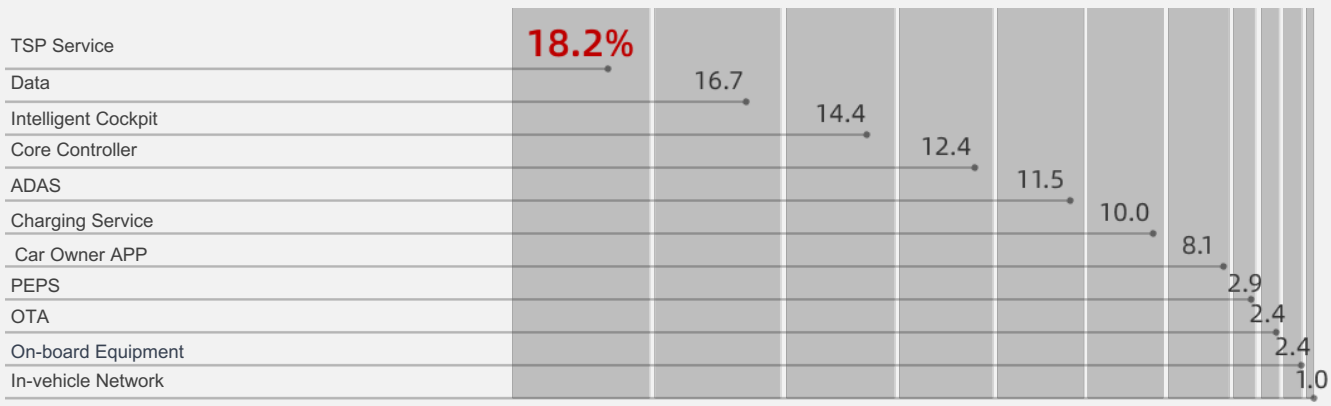
In recent years, with the rapid development of smart car technology, attacks on smart cars have gradually shifted from traditional attacks on single vehicle controllers to attacks on entire vehicle intelligent services. This includes, but is not limited to, manipulation of remote control applications, penetration of cloud services, cracking of intelligent cockpit systems, and attacks on third-party applications and intelligent services.

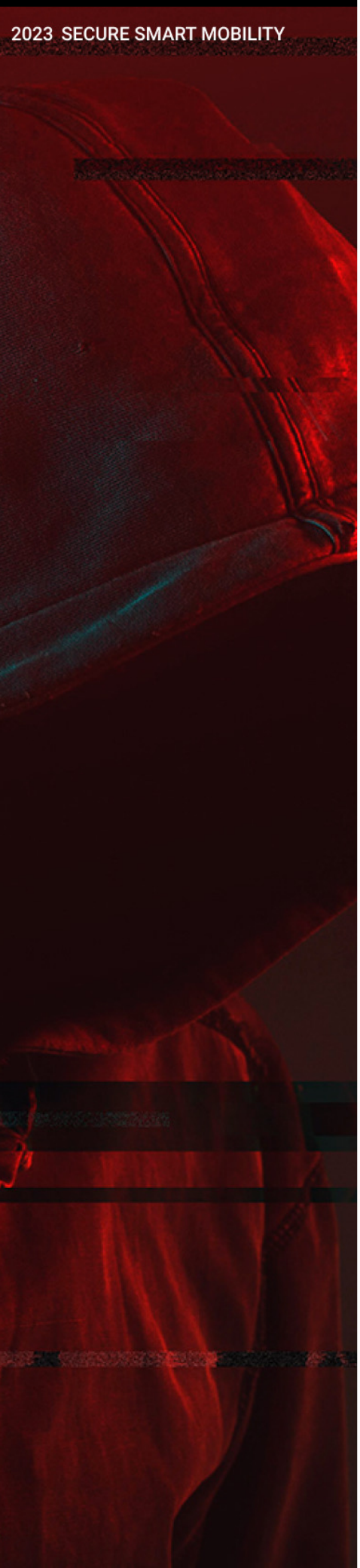
With the compliance requirements of WP.29 R155&R156, car companies have established comprehensive cybersecurity management systems to ensure vehicle safety throughout their lifecycle. Despite this, an increasing number of vulnerabilities in intelligent services are being exposed, affecting the safety of smart cars.

Automotive Vulnerability Percentage in 2023



Percentage of car safety incidents in 2023





Ongoing Threats

TSP service threats

The Callisto Threat Intelligence Center analyzed automotive vulnerabilities since 2023, and we found that 47.5% of the vulnerabilities are related to TSP services. Among the known automotive vulnerabilities, those related to TSP services mainly involve cloud configuration errors, cloud token leakage, authentication mechanism bypass, API permission abuse, etc. Attackers can exploit these vulnerabilities to achieve remote control of a single vehicle, and even realize batch control of vehicles.

Intelligent cockpit threats

In 2023, the intelligent cockpit continues to be a subject of ongoing research by experts, who have found multiple vulnerabilities related to the intelligent cockpit. These include bypassing the signature mechanism of the vehicle infotainment firmware updates to implant malicious backdoors into the system; causing the player to crash by fuzz testing the vehicle infotainment audio decoder; gaining control over the vehicle infotainment system through heap overflow vulnerabilities and out-of-bounds write vulnerabilities in Bluetooth chip modules; and using voltage fault injection to bypass secure boot and obtain Root access to the vehicle infotainment system.

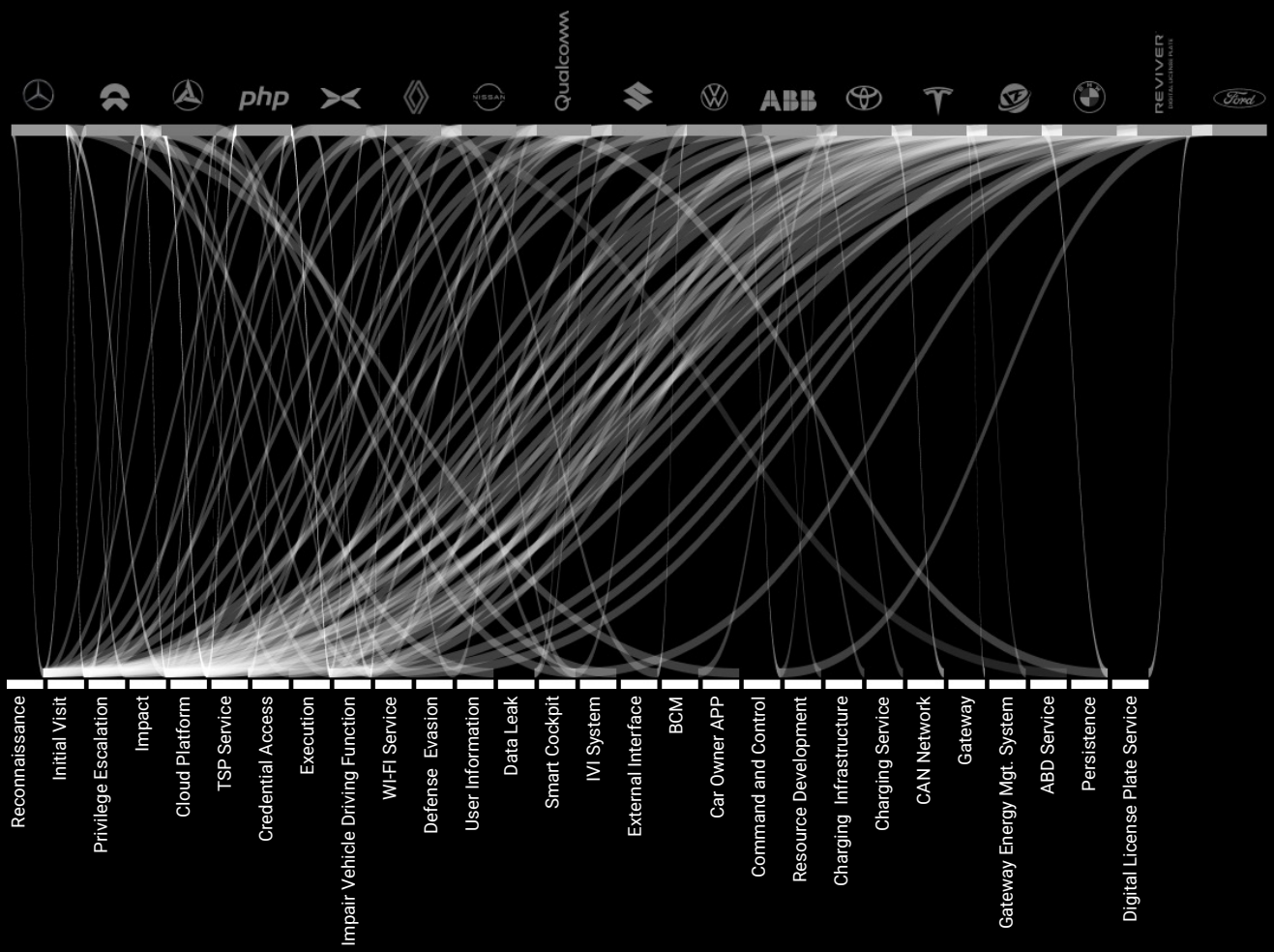
Charging service threats

As electric vehicles (EVs) become more prevalent, the cybersecurity of charging stations becomes particularly important. Currently, charging services mainly face the following four threats: First, remote interference vulnerabilities, such as the "Brokenwire" vulnerability, which can remotely disrupt the charging of a large number of EVs; second, protocol exploitation attacks, using attacks launched through the Open Charge Point Protocol (OCPP), which may lead to denial-of-service attacks on charging points; third, unauthorized access, involving unauthorized access to charging station systems, which may threaten data security; and fourth, remote takeover threats: exploiting vulnerabilities in Bluetooth Low Energy (BLE) technology to achieve remote takeover of chargers.

Car owner APP threats

As an intelligent application for remote vehicle control and real-time monitoring of vehicle status, the car owner APP faces an increasing number of threats. Based on the analysis of automotive vulnerabilities and security events tracked in 2023, the existing threats involve three types: The first is the remote control threat, where attackers exploit API vulnerabilities to achieve remote control of the vehicle, including unlocking doors, starting the engine, or even intervening in vehicle driving; the second is account security risk, where the car owner APP accounts may be attacked by attackers who use stolen accounts to control the vehicle; the third is data privacy leakage, where the data collected by the car owner APP may contain sensitive information, such as location data and driving habits. If this data is accessed or misused improperly, it could lead to serious privacy issues.

2023 Automotive Attack Incidents



Mercedes
An access control issue in Mercedes me IOS APP v1.34.0 and below allows an attacker to view other users' maintenance orders and access sensitive user information via unspecified vectors.

NIO
NIO cars have misconfiguration and directory traversal vulnerabilities, which can escalate privileges to Root.

Toyota
'Headlight hackers' steal cars via CAN jamming.

phpscriptpoint
phpscriptpoint Car Listing 1.6, the Car Listing Content Management System (CMS), is vulnerable to (CVE-2023-3858 and CVE-2023-3859).

ABB
Vehicle charging platforms face threats of theft .

Renault
Renault Zoe EV 2021 car infotainment system USB vulnerability.

Nissan
Nissan's Australia and New Zealand operations have been hit by a cyberattack.

Qualcomm
Improper access control in the automotive operating system platform Android.

Suzuki
Suzuki Motors leaks sensitive information.

Volkswagen
There is a vulnerability in Volkswagen's IVI system.

Sany Heavy Industry
The ASRG-China community discovered extremely critical vulnerabilities in the T-BOX of companies such as Sany Heavy Industry.

Tesla
Tesla gateway suffered TOCTTOU attack.

Yanfeng
Yanfeng was attacked by the "Kirin" ransomware, causing production interruption at its North American factory.

BMW
Complete account takeover of BMW and Rolls Royce via misconfigured SSO.

Reviver
California's new digital license plates were hacked.

Ford
Ford says cars with Wi-Fi vulnerabilities are still safe to drive.

Xpeng Motors
Xpeng Motors turns on the developer mode to enable arbitrary installation of APPs.

Solutions for Diverse Attacks

Deepen Business Understanding

Automotive security teams further understand the company's different models' Electrical/Electronic Architecture (EEA) and software architecture, as well as the services provided to the outside, by establishing security baselines, designing security architectures, VTA verification, and security operations.

Enhance Professional Skills

Starting with core automotive assets and intelligent services, senior security researchers need to quickly transition from traditional IT attack and defense methods to technical research on automotive cybersecurity.

Introduce Targeted Threat Monitoring Platforms

Accelerate the integration of vehicles with specialized security monitoring and operation platforms (VSOC), leveraging the capabilities of cloud computing and AI to quickly mitigate harm when widespread threats arise, a measure that can greatly reduce the brand risk caused by threats.

Join Communities

Assigning personnel to join automotive cybersecurity communities can enhance the enterprise's perception of risks.

Case Study - ADAS Domain Controller Threats

With the enhancement of assisted driving functions, ADAS domain controllers inevitably expose multiple potential attack surfaces. Attack methods include: transient injection attacks on low-power CAN buses, misleading attacks on sensor signals, destructive code injections via backend management interfaces, and direct manipulation of vehicle behavior through control commands. More seriously, these attacks could exploit the vehicle's functional safety features, impacting driving safety.

initial access

Attackers used nmap to scan a sub-device of the domain controller and found that port 22 was open, then used brute force to crack the correct login password.

Persistent command execution

The attacker transmitted a reverse connection script constructed with telnet commands through the debugging port and, after opening the reverse connection, obtained remote execution privileges.

functional destruction

The attacker killed the autonomous parking service process using the kill command, causing this autonomous parking function to fail and the system to restart.

functional destruction

After obtaining root access to the domain controller, attackers may locate and terminate the existing positioning service process and replace it with a malicious program, resulting in the failure of the vehicle's RTK high-precision positioning service. This could adversely affect navigation and driving safety.

command execution

The attacker logged into the domain controller sub-device through the debugging port, viewed its running processes with the ps -A command, guessed its main function through the process name, and used the scp command to upload sensitive files.

Lateral movement

The attacker uploaded the nmap tool to the domain controller and used this tool to scan the network. They discovered two IP addresses with port 22 open. Through brute force with BrutesPray, they cracked the login credentials. Ultimately, they used port 22 to log into a device within one of the IP subnets on the internal network.

Lateral movement

The attacker uses port 22 to log in to another IP subnet device in the intranet.

Case Study

PEPS Threat

The Callisto Automotive Threat Intelligence Center has discovered that the main attack methods against smart cars in 2023 include Bluetooth Low Energy (BLE) relay attacks, RF replay attacks, CAN injection, and bypassing of anti-theft technologies. Particularly, the attack method of relaying at the Bluetooth link layer, proposed by NCC last year, is effective against most Bluetooth car keys currently on the market.

BLE link layer relay

The Callisto Automotive Threat Intelligence has detected thieves using Bluetooth link layer relay devices to steal cars. The relay device forwards the link layer PDUs and controls the connection event intervals to carry out the relay operation. The cunning aspect of this attack lies in the fact that it goes undetected by the victim's iOS or Android application layer, and Bluetooth link layer encryption is also unable to resist this attack.

RF playback& No anti-theft technology

According to data from the Intelligence Center, in recent years, there have been frequent incidents of radio frequency signal man-in-the-middle attacks, and to this day, older car models still have a probability of lacking anti-theft and being susceptible to RF key replay attacks.

CAN injection

Tracking through the dark web has revealed a physical theft method where thieves dismantle the headlights to access an emergency start device purchased at a high price on the dark web, and send CAN messages to unlock the vehicle. The digital key ECU of the stolen vehicle and the headlight ECU are on the same CAN network, and due to the broadcasting nature of the CAN bus, the vehicle executed commands to disable the anti-theft and open the doors.

Anti-theft bypass

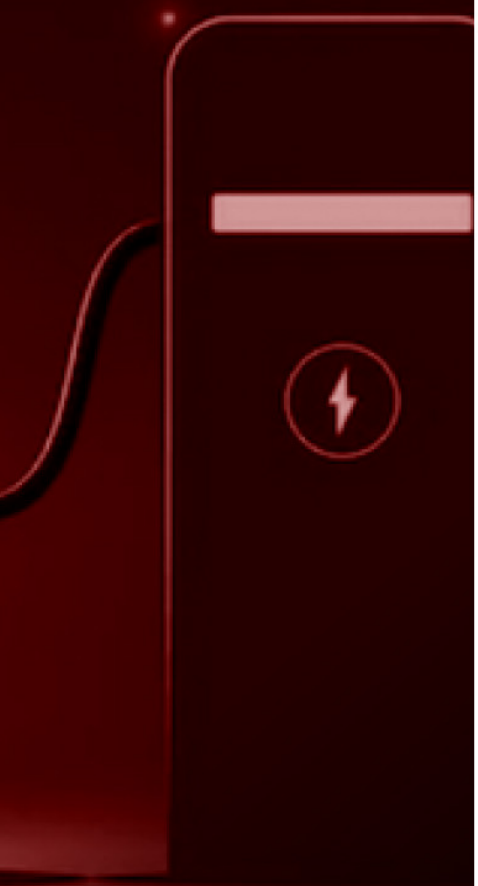
In 2023, a large number of modern Hyundai and Kia vehicles in the United States still did not use anti-theft technology, allowing thieves to start the engine simply by inserting a USB into the ignition device. As a result, the Hyundai Motor Group has recalled nearly 4 million vehicles. The Callisto Automotive Threat Intelligence Center reminds the industry that current domestic and international regulations require automakers to ensure the safety of the vehicle's entire lifecycle. Automakers should widely apply OTA technology and VSOC security operations to ensure continuous updates and maintenance for sold vehicles.

Influence

The Callisto Automotive Threat Intelligence Center predicts that relay attacks will continue to be the main method used by car thieves for three reasons: First, due to the widespread application of anti-theft technology, replay attacks or rolling code attacks can only open car doors and cannot start the engine, which does not achieve the thieves' goal. Second, the cost of relay devices is low, and if circulated on the dark web, it can generate a significant profit. Third, relay attacks do not require expert-level attackers like bypassing checks or exploiting hardware vulnerabilities do; relay devices are simple to use, making it easy for thieves to operate.

Case Study

Charging Pile Threat



Charging Infrastructure Threats

Denial of service and data leakage caused by charging piles

In February 2023, vulnerabilities in the OCPP 1.6 protocol drew widespread attention within the industry. According to the security extension of the OCPP 1.6J version of the protocol standard, three methods of authentication are supported when charging piles verify their identity with the Central System Management System (CSMS): charging pile identification only, charging pile identity and credentials, and charging pile identification with client certificates. When only charging pile identification is used for authentication, it may lead to a DOS attack on the charging station. Attackers may exploit the time difference when a legitimate charging pile reconnects to the CSMS to steal energy or obtain sensitive information from the charging pile and further misuse it.

Attackers can combine the leakage of charging station information to further expand the impact—hackers can search for the installation manual of the operator's OCPP terminal on search engines, obtain the operator's service URL, or search for the operator's charging service website and discover related identifiers through the data exposed by the website API. The combination of the above information leakage can cause large-scale charging stations to suffer from the impact of OCPP protocol authentication bypass issues.

Researchers have been dedicated to the security study of charging infrastructure, and since 2020, several charging infrastructure issues have been discovered. Typical security issues include the hard-coded vulnerabilities of the Schneider charging pile web backend, firmware verification algorithm defects that allow malicious firmware to be flashed to gain root access to the charging pile, and the GB/T 27930 protocol vulnerability between the non-sensing payment charging pile and the battery management system that leads to energy theft. The charging infrastructure is prone to logical issues and improper verification problems in communication protocols due to the involvement of multiple organizations and the complexity of inter-organizational communications.

OEM - VCSI

Vehicle Cybersecurity Index

With the rapid development of intelligent connected vehicle technology, cybersecurity has become an important consideration for various car manufacturers. The OEM-VCSI (OEM Vehicle Cyber Security Index) aims to assess the complex and evolving state of automotive manufacturers in terms of cybersecurity.

Commercial OEM and Tier 1 suppliers can rely on the VCSI as an assessment mechanism, evaluating their investment and deficiencies in automotive cybersecurity from a 0-10 point perspective.

Vehicle Cybersecurity Index

Personnel Structure

There are issues with immature team configurations, with functional safety still doubling up as cybersecurity in some cases. 40% of OEM companies have completed the transition to complex personnel configurations composed of senior automotive security experts and automotive engineers.

Investment Budget

The average proportion of the cybersecurity budget in the total R&D budget for automotive is 2%, which is far below traditional cybersecurity. This is particularly concerning given the increase in cyber threats and the complexity of intelligent automotive systems.

Security Baseline

Automotive companies are increasingly focusing on regulatory compliance and standards, such as WP.29 and ISO/SAE 21434, which emphasize the basic standards of cybersecurity practices. About 40% of companies have started to transition towards establishing a cybersecurity baseline for automobiles.

EEA Understanding

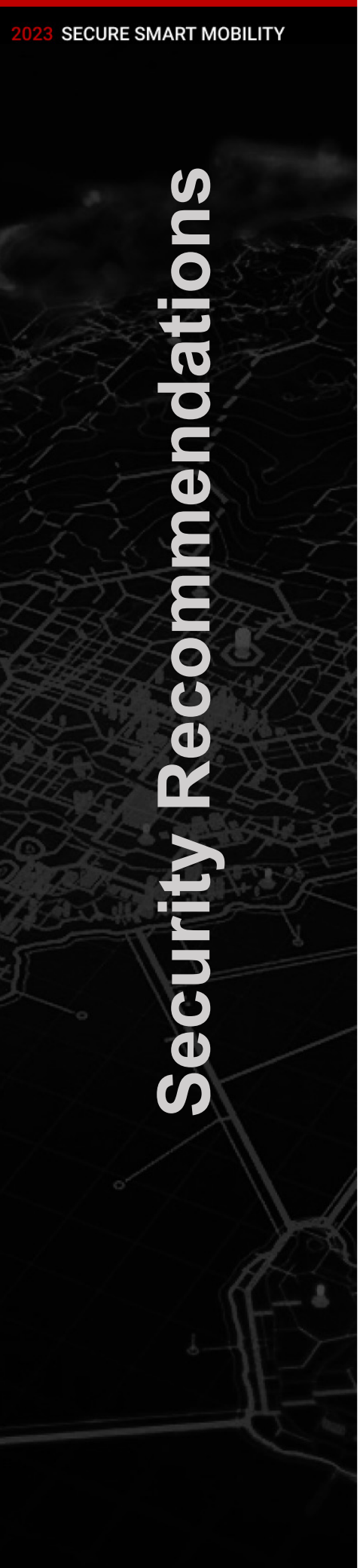
The importance of cybersecurity for intelligent vehicles is reflected in protecting vehicles from external attacks and maintaining the safety of drivers and passengers. This requires an in-depth understanding of core assets in the automotive EEA and intelligent services. Currently, 20% of company security teams have begun to delve deeply into business processes and design decisions.

Operational Capability

Currently, 90% of automotive companies are not yet ready for efficient cybersecurity operations. The introduction of the Vehicle Security Operations Center (VSOC) represents the development of industry operational capabilities, offering a more comprehensive and integrated approach to cyber risk management, but the security response for millions of vehicles is still in need of accumulation and refinement.

Innovative Technology

Automotive companies show high enthusiasm for dealing with new types of cyber threats, such as remote vehicle control vulnerabilities and attacks on electric vehicle charging infrastructure. Innovative technologies are needed to address these new challenges, with about 50% of companies having clear target investments and planning trends in 2023."



Security Recommendations

Five Measures

01

Deep Understanding of Core Assets and Intelligent Services

Automotive cybersecurity strategies need to start from the perspective of core assets and intelligent services, conducting system-level asset identification, including key components of in-vehicle networks, control systems, and data storage. At the same time, analyze the data flow and dependencies of intelligent services to identify potential security risk points and develop corresponding security strategies.

02

Continuous Vulnerability Assessment and Supply Chain Threat Intelligence Sharing

Regularly perform system-level vulnerability scans covering all critical components of the vehicle. At the same time, share security information with suppliers, including known vulnerabilities and patches, to ensure the security of the entire supply chain. Participate in threat intelligence sharing platforms to obtain and share the latest security threat information.

03

Consideration of Cloud Services and Strategy Deployment

Leverage the elasticity and security advantages of cloud computing to integrate cloud services into vehicle systems, such as using cloud services for big data analysis and threat monitoring.

The application of artificial intelligence in anomaly detection and automated response will be an important direction for the future development of VSOCs.

04

Understanding Attackers and Conducting Simulation Drills

Through continuous threat intelligence and attack pattern analysis, understand potential attackers and methods of attack.

Regularly organize red team attack simulations and blue team defense drills to test the effectiveness of security strategies in a practical way.

05

Continuous Improvement of Skills and Knowledge

Encourage automotive security engineers to not only delve into technical details but also understand how these technologies integrate with business objectives and intelligent vehicle services.

Explore and learn about the application of emerging technologies such as artificial intelligence, large language models, and domain control edge computing in cybersecurity.

VSOC - Vehicle Security Operations Platform

Continuous Monitoring and Response

Conduct continuous monitoring of the core assets of vehicles and intelligent services, monitoring different temporal sensors, ECU instructions, MCU operations, network operations, system operations, applications, and data. The granularity can be refined to the manipulation behavior of different users and different vehicles.

AI Detection of Unknown Threats

Utilize twin technology to establish a security model for vehicles, cross-analyze the state of vehicles in the physical and digital worlds, and combine machine learning to achieve anomaly analysis of unknown attacks.

Advanced Automated Analysis

Comprehensively acquire and automatically analyze up to 200 items of automotive abnormal events according to anomaly event templates, and trace back to the granularity level of network packet content, vehicle control instructions, API commands, etc.

Globally Visiblility and Control

Automatically adaptable drag-and-drop global big screen, customize the monitoring information for different screens, covering dozens of dimensions such as network security, system security, online services, abnormal status, supply chain information, etc., for a display overview.

VTI - Vehicle Threat Intelligence

Intelligent vehicle threat intelligence and vulnerability management solutions. The product focuses on collecting, analyzing, and publishing threat intelligence in the automotive industry, and provides tailored automotive threat intelligence services for automakers, Tier 1 suppliers, connected car service providers, fleets, etc.

Vulnerability Full Lifecycle Management Mechanism

Supports the management of the full lifecycle of vulnerabilities including vulnerability monitoring, identification, analysis, repair, and validation.

Multi-Source Vulnerability Intelligence Data Fusion

Supports the fusion of multi-source threat intelligence data such as public vulnerabilities, supply chain vulnerabilities, public news reports, the deep web/dark web, automotive forums, academic research, automotive white hat/security teams, and automotive vulnerability mining.

Vulnerability Priority Assessment Technology

Supports the assessment of automotive vulnerability priorities, effectively allocates resources, and minimizes potential security risks to the greatest extent.

WP.29 R155 Gap Analysis

Supports compliance gap analysis and produces compliance gap analysis reports, providing customized reports for automakers and suppliers.

VDR Automotive Domain Control Information Security Solution

Communication and Network Security

Supports secure external connections to the domain controller and secure communication protocols within the domain.

Operating System Security

Supports detection of system security events, security configuration, and anomalies in operational status.

Anomaly Detection and Monitoring

Supports vulnerability detection, sensitive file monitoring, and application detection.

Sensitive Data Security

Provides an encryption SDK for sensitive data and critical logs.

About us

卡卫星科技
CALLISTOTECHNOLOGY

Callisto was founded by one of the first groups of global technical experts focused on automotive cybersecurity. Thanks to years of accumulation in the field of automotive cybersecurity, we are able to start from a perspective of combined offense and defense, integrating advanced artificial intelligence and knowledge graph engine capabilities. By algorithmic analysis of the massive amount of heterogeneous messages, instructions, and API services from connected vehicles, we can defend against new types of connected vehicle attacks targeted at automakers and supply chains. We provide threat awareness and defense capabilities for intelligent connected vehicles, protecting the safety of core automotive assets and intelligent services.

We maintain a great passion and interest in the automotive and cybersecurity industries. At the same time, we respect and fully learn from the engineering experience and industry practices of the automotive industry over the years, committed to providing enterprises with more professional and leading security products and services. Callisto emphasizes the full release of data value, while highlighting the combination of scientific analysis methods and practical application services. We profile the vehicle's security status from multiple perspectives, automatically analyze anomalies and manage risks, enrich analysis dimensions, and reduce the operational pressure on security personnel."

Callisto Technology Co., Ltd.

Website：https://www.callisto-auto.com

Email：contact@callisto-auto.com

Reference

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/