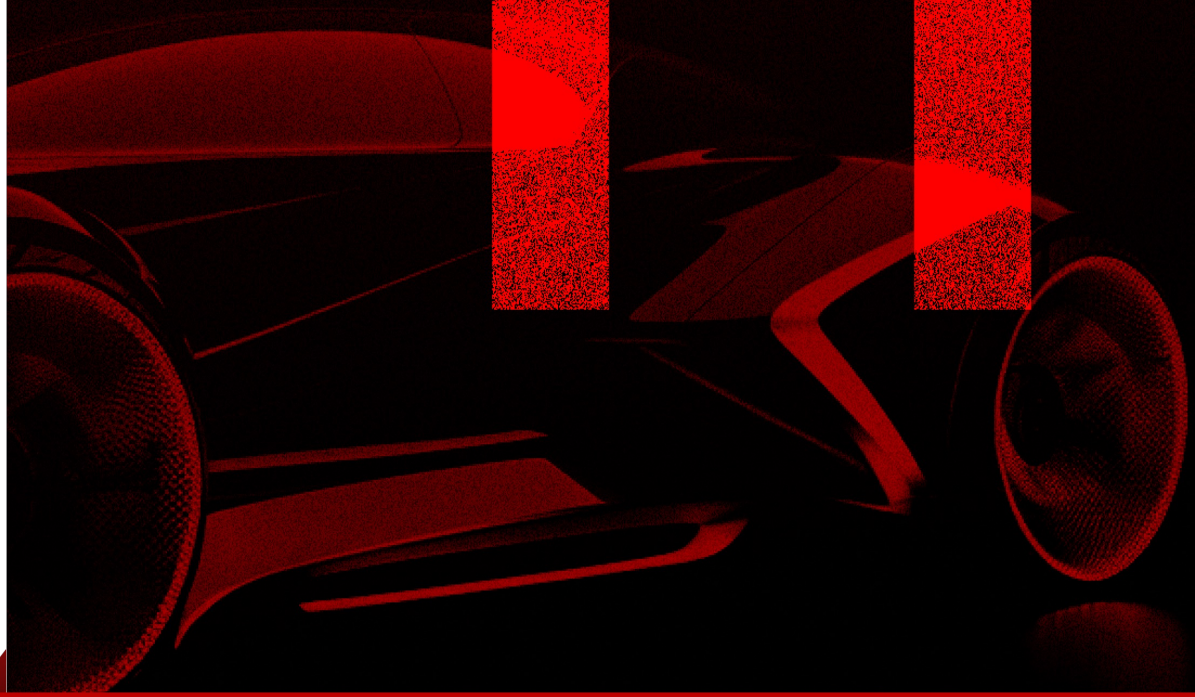
木卫四科技
CALLISTOTECHNOLOGY

H1



2024 Semi-annual

Automotive Vulnerability and Threat Intelligence - Briefing

With the rapid development of smart car technology, its cybersecurity issues have increasingly become the focus of the industry. Threat intelligence distribution statistics in the first half of 2024 show that the security situation in the field of smart cars is becoming increasingly severe.

32%

Vulnerability intelligence

Vulnerability intelligence covers remote attacks, near-field attacks, and local attacks, etc.

68%

Cybersecurity incident intelligence

cybersecurity incident intelligence occupies the main part, involving data leaks, data tampering, malware attacks, wireless network intrusions, etc.

The sources of smart car threat intelligence in this report are diverse, and each source provides us with a unique perspective and data, helping us build a multi-dimensional threat intelligence system and enhance our understanding of smart car cybersecurity risks.

The proportion of smart car safety incidents published by mainstream news media and automotive ecological communities is as high as 60%, which has reached a proportion worthy of attention and reflects the public's increasing concern for smart car cybersecurity issues.

60%

Mainstream news media, automotive ecological community

32%

Vulnerability platform

The proportion of Internet of Vehicles vulnerabilities announced by the vulnerability platform is closely followed, further highlighting the urgency of strengthening smart car cybersecurity protection.

6%

Social media

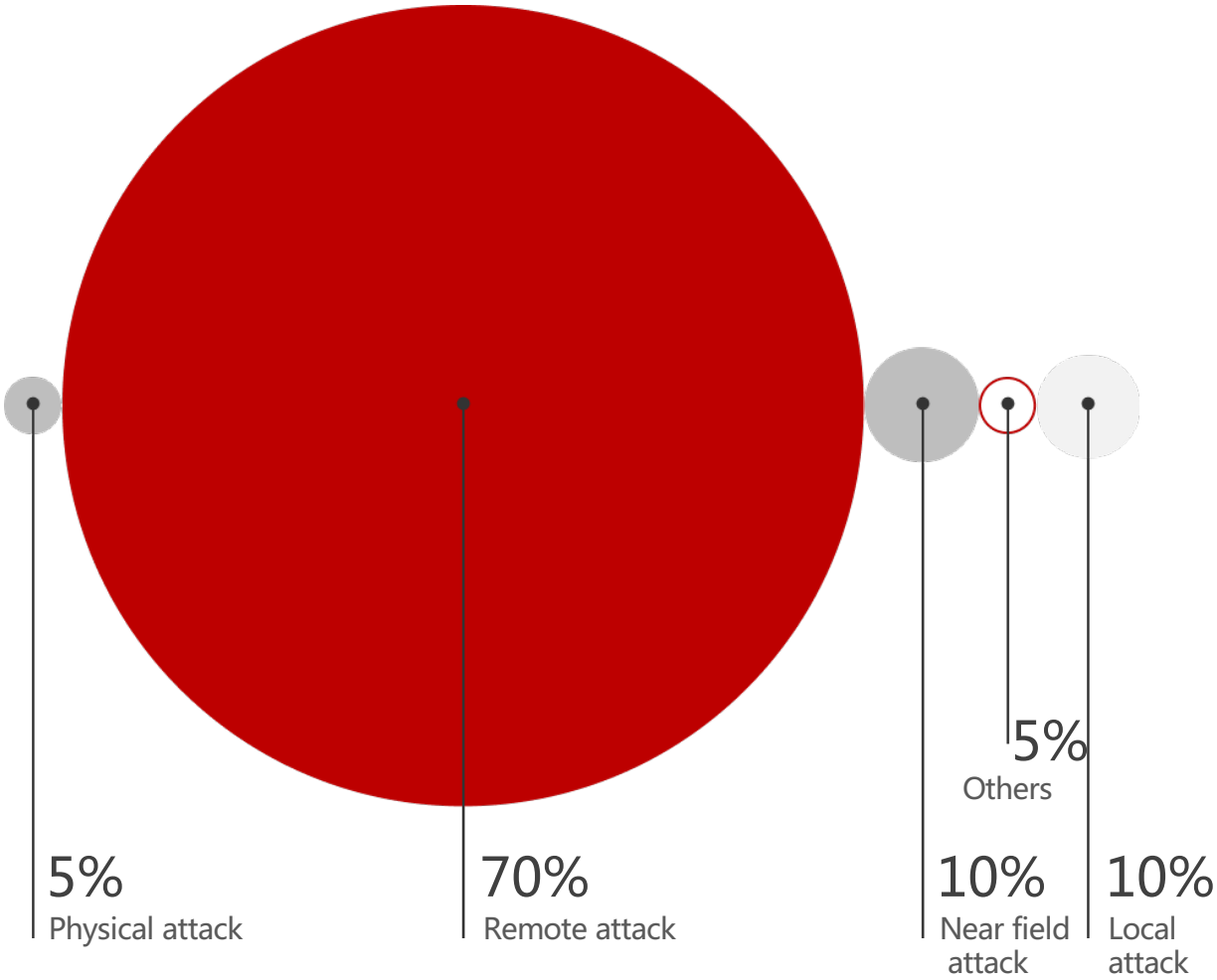
1%

Security blog

1%

Security meeting

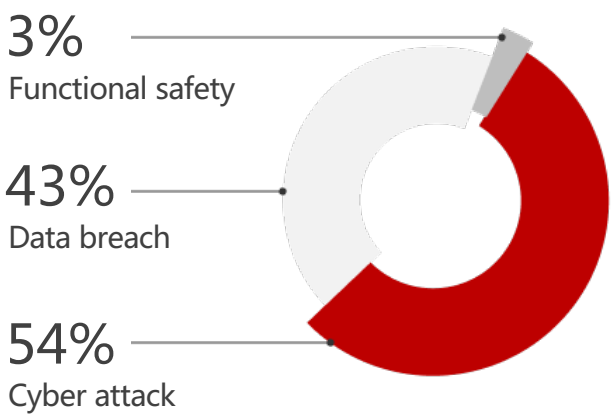
Attack vector analysis



In the first half of 2024, smart car faced a variety of attack vectors, covering remote, near-field, local, physical and other forms of attacks. In-depth analysis of these attack vectors can help understand attackers' methods and strategies, so as to develop more effective defense measures.

Event type analysis

In the first half of 2024, the smart cars faced a wide variety of security incidents. Cyber attacks, data leaks and functional safety incidents each present unique threat characteristics. According to statistics, network attacks account for the largest number of incidents, accounting for 54% of all security incidents.



Security incident

January

Hard-coded UDS service credentials exist in the firmware of Skoda Auto's MIB3 infotainment system, exposing key secret values. These hard-coded credentials, including passwords and encryption keys, are used for inbound authentication of the system, outbound communication with external components, and encryption of internal data.

Mercedes-Benz's internal data is at serious risk of leakage after an employee accidentally leaked code warehouse credentials. The credentials provide unrestricted access to the company's GitHub Enterprise Server, allowing anyone to download the company's private source code repository.

February

Due to a misconfiguration, a Microsoft Azure storage server (i.e. "bucket") in BMW's development environment was accidentally exposed to public access. The bucket contained script files that exposed Azure container access information, keys used to access private buckets, and other cloud service details.

Nissan's luxury brand Infiniti USA was attacked by the Mogilevich ransomware group, resulting in the leakage of 22GB of sensitive data including vehicle identification numbers, customer names, addresses, emails and passwords.

March

Security researchers have discovered a phishing attack method that fakes Tesla's official WiFi and login interface, tricking car owners into entering account credentials, thereby activating the mobile key and taking full control of the vehicle.

Colorado State University researchers have discovered a critical vulnerability in the electronic logging devices (ELDs) of U.S. commercial trucks that could be controlled by attackers via Bluetooth or Wi-Fi and spread worm attacks

April

An unauthorized access vulnerability exists in a Spanish charging equipment company's electric vehicle charger, allowing an unauthorized attacker to access sensitive information via a network interface.

Honda Vietnam's database was leaked on a hacker forum, and the leaked information included sensitive information such as customer ID numbers, phone numbers, vehicle types and purchase details.

May

Security researchers have discovered that Tesla Model 3 has a gateway firmware signature verification bypass vulnerability that allows network-adjacent attackers to execute arbitrary code on the vehicle.

Nissan North America recently suffered a data breach that exposed the personal information (including names and Social Security numbers) of more than 53,000 current and former employees.

A security vulnerability exists in the default credentials of Italian electric vehicle charging equipment. An attacker exploiting this vulnerability could lead to device disabling, payment bypass, or payment data access.

June

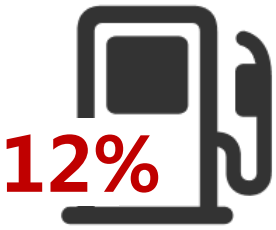
Security researchers have discovered a resource exposure vulnerability in Schneider Electric charging piles that allows an attacker to perform a denial of service attack through remote port scanning and fingerprinting without authentication.

CDK Global suffered a cyber attack that forced the suspension of sales operations at approximately 15,000 U.S. auto dealers, including General Motors dealers and Group 1 Automotive, which has hundreds of dealerships.

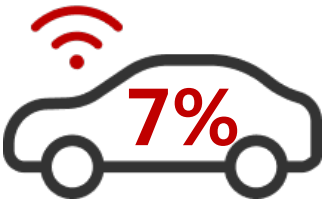
There is a serious security vulnerability in a certain vehicle management system, which may be exploited for remote attacks.

Intelligent function threat coverage

Smart cockpit The threat risks that occur mainly focus on infotainment systems and user interfaces

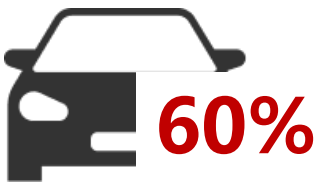


Smart charging service The threat risks that occur mainly focus on charging stations and charging communication protocols.



Intelligent vehicle control The threat risks that occur mainly focus on vehicle remote control and driver assistance systems

Intelligent driving The threat risks that occur are mainly concentrated in autonomous driving systems



Other Scenarios The risks that occur mainly focus on TSP services and privacy data

Analysis of affected assets

Security incidents in the field of smart cars have had widespread and far-reaching impacts on a variety of critical assets. These assets include sensitive data, charging services, TSP services (remote service platform), smart cockpits and many other important areas. Below is a detailed analysis of how different assets are affected.

As the data collection and on-board functions of smart cars continue to expand, sensitive data and security issues have become particularly serious.

The security issue of sensitive data is particularly prominent, accounting for as high as 47% of all security incidents. These incidents often include risks such as data breaches and data tampering, posing serious threats to personal privacy and corporate confidentiality. Following closely, TSP services and smart cockpit systems have also become the main targets of cyber attackers.

47% Sensitive data

14% TSP

13% Smart cockpit

The popularity of smart electric vehicles makes the safety of charging infrastructure critical.

14%

Charging service Attackers affect vehicle charging security and charging efficiency by invading the charging station control system or exploiting charging communication protocol vulnerabilities.

Security incidents in the field of smart cars have had serious and far-reaching impacts on a variety of critical assets. These assets include smart keys, in-vehicle equipment, in-vehicle networks, ADAS systems, etc.

6%

ADAS Systems

Attackers invade the ADAS system, obtain control permissions or tamper with system data, affecting the autonomous driving function and causing driving risks.

3%

Smart keys

As a core component for vehicle access and starting device, smart keys may face the risk of cloning and illegal access in security incidents, threatening the physical security of the vehicle.

2%

In-vehicle network

The vehicle network is the link connecting the electronic control units of the vehicle. Once attacked, it may cause vehicle control failure and even cause a safety accident.

1%

Vehicle equipment

When in-vehicle devices such as in-vehicle information systems, navigation equipment, and entertainment systems are attacked, they may not only leak user data, but may also affect the normal functions and driving experience of the vehicle.

About Us

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.

About S3-VTI

S3-VTI The Callisto Automotive Threat Intelligence Platform is tailor-made for automobile manufactures and supply chain systems, providing comprehensive automotive-specific threat intelligence, event tracking, vehicle vulnerability detection, threat impact analysis and mitigation recommendations. As the first domestic threat intelligence and vulnerability management solution designed specifically for the intelligent connected vehicle ecosystem, the S3-VTI platform is dedicated to collecting, analyzing and publishing threat intelligence in the automotive industry, for automobile manufacturers and first-tier suppliers (Tier 1) , second-tier suppliers (Tier 2) and connected car service providers and other market segments, providing customized automotive threat intelligence services.

Callisto Technology

Website：https://www.callisto-auto.com

Email：contact@callisto-auto.com