SECURITY
DAYS

KIBERNETINIO SAUGUMO KONFERENCIJA

Rugsėjo 7 d. 2023

esd.eset.lt

SECURITY DAYS

AR ATEITYJE GALĖSIME SAUGIAI JAUSTIS SAVO PAČIŲ AUTOMOBILIUOSE?

Agnė Marija Bučytė - automobilių kibernetinio saugumo specialistė

Rugsėjo 7 d. 2023

KIBERNETINIO SAUGUMO KONFERENCIJA

Ateitis jau yra dabar

2017

2018

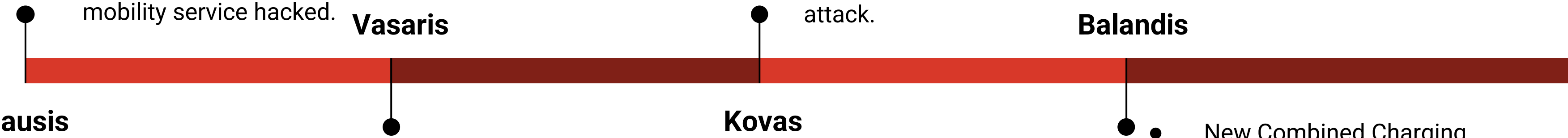
2019

2021

2022

2023

Top 2022 metų incidentai



Sausis

- Hacker remotely controls 25 American OEM EVs around the world.
- Several vulnerabilities were found in multiple charging stations which allowed remote attackers to impersonate charging station admin users and carry out actions on their behalf.
- App account of American mobility service hacked.

Vasaris

- Russian electric vehicle chargers were hacked and disabled by a Ukrainian EV charging parts supplier as part of a cyberwar effort.
- Cyber attack on a Japanese OEM’s supply chain shuts down 14 factories in Japan for 24 hours.
- Tier-2 company hit by cyber attack.

Kovas

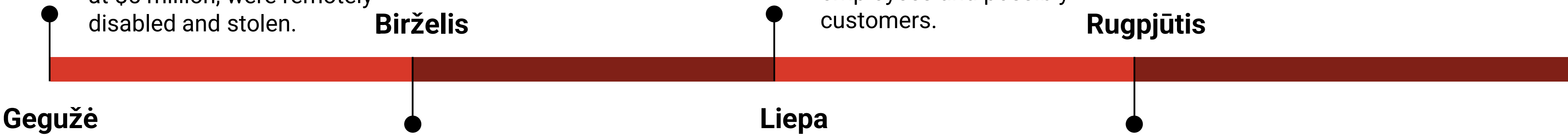
- OEM-affiliated supplier hit by cyber attack.
- Two major OEMs vulnerable to replay attacks let hackers remotely unlock and start vehicles.
- Italian railway firm falls victim to ransomware attack.

Balandis

- New Combined Charging Stations (CCS) attack technique found with the potential to disrupt the ability to charge electric vehicles at scale.
- Automotive tools manufacturer discloses data breach claimed by Conti ransomware gang.

Šaltinis: Upstream 2023 Global Automotive Cybersecurity Report

Top 2022 metų incidentai



Gegužė

- Chinese OEM vehicles were found to be vulnerable to attacks via update processes.
- German automakers targeted in a year-long malware campaign.
- Agriculture vehicles, valued at $5 million, were remotely disabled and stolen.

Birželis

- Hackers targeted vehicles of an American OEM through Bluetooth attacks.
- Eight zero-day vulnerabilities discovered in a popular industrial control system used in the transportation sector.
- Japanese automotive supplier hit by ransomware attack.

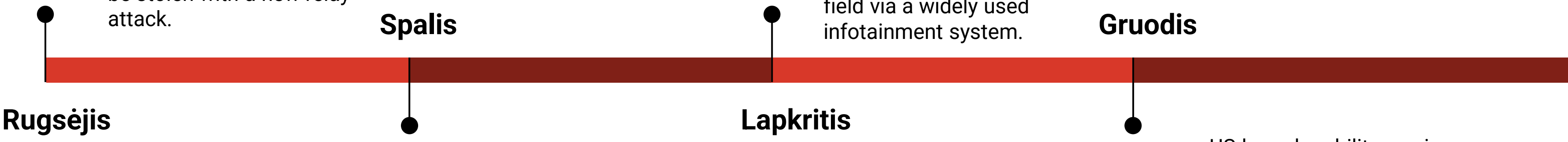
Liepa

- A hacker gained control over a head unit of Japanese automotive through the dashboard’s API.
- Popular vehicle GPS tracker gives hackers admin privileges.
- Car rental firm experiences a data breach, affecting employees and possibly customers.

Rugpjūtis

- Three ransomware attacks were launched against a Tier-1 supplier.
- A new mobile app vulnerability was discovered, enabling man-in-the-middle attacks on EV OEMs.
- North American automotive dealership affected by data breach.

Top 2022 metų incidentai



Rugsėjis

- Hackers attacked a popular taxi app, causing massive traffic jams.
- American moving and storage rental company impacted by data breach.
- Vehicles of American OEM can be stolen with a new relay attack.

Spalis

- Italian OEM hit by ransomware attack.
- Japanese OEM customers affected by data breach in its mobile app.
- UK car retail giant hit by ransomware attack.

Lapkritis

- A ransomware group offered all information stolen from a global Tier 1 supplier, in a ransomware attack, for sale on the dark web for $50 million.
- Cyber attack shuts down Denmark’s largest train company.
- White hat hackers remotely started, stopped, locked, and unlocked vehicles of multiple OEMs by sending API requests with the VIN on a unique ID field via a widely used infotainment system.

Gruodis

- US-based mobility service provider impacted by a data breach at a 3rd-party vendor used for asset management.
- Chinese EV OEM impacted by a data breach and ransomware demand of $2.25 million in Bitcoin.

Nuo ko viskas prasidėjo?

Koks yra žymiausias automobilių kibernetinio saugumo incidentas?

Nuo ko viskas prasidėjo?

Koks yra žymiausias automobilių kibernetinio saugumo incidentas?

Nuo ko viskas prasidėjo?

Koks yra žymiausias automobilių kibernetinio saugumo incidentas?

Charlie Miller

Chris Valasek

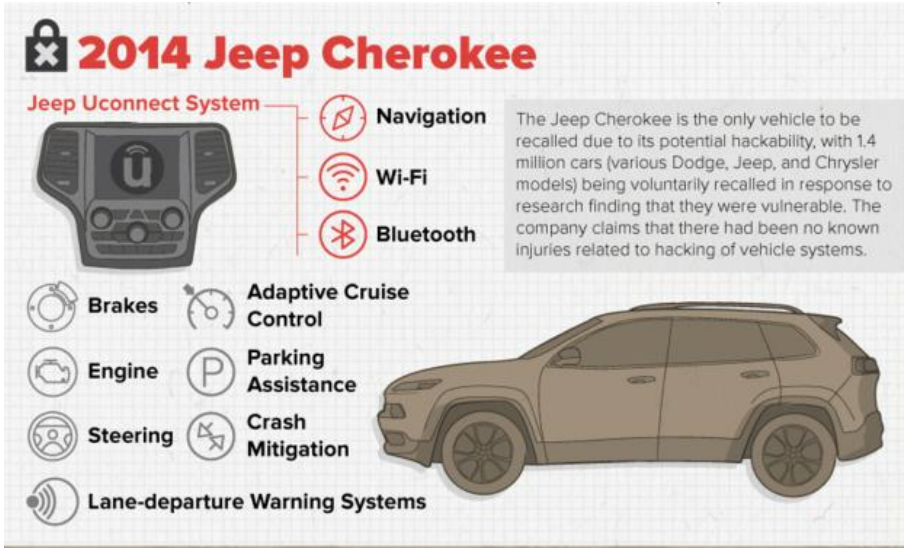
Jeep incidentas

Kada: 2015 metais

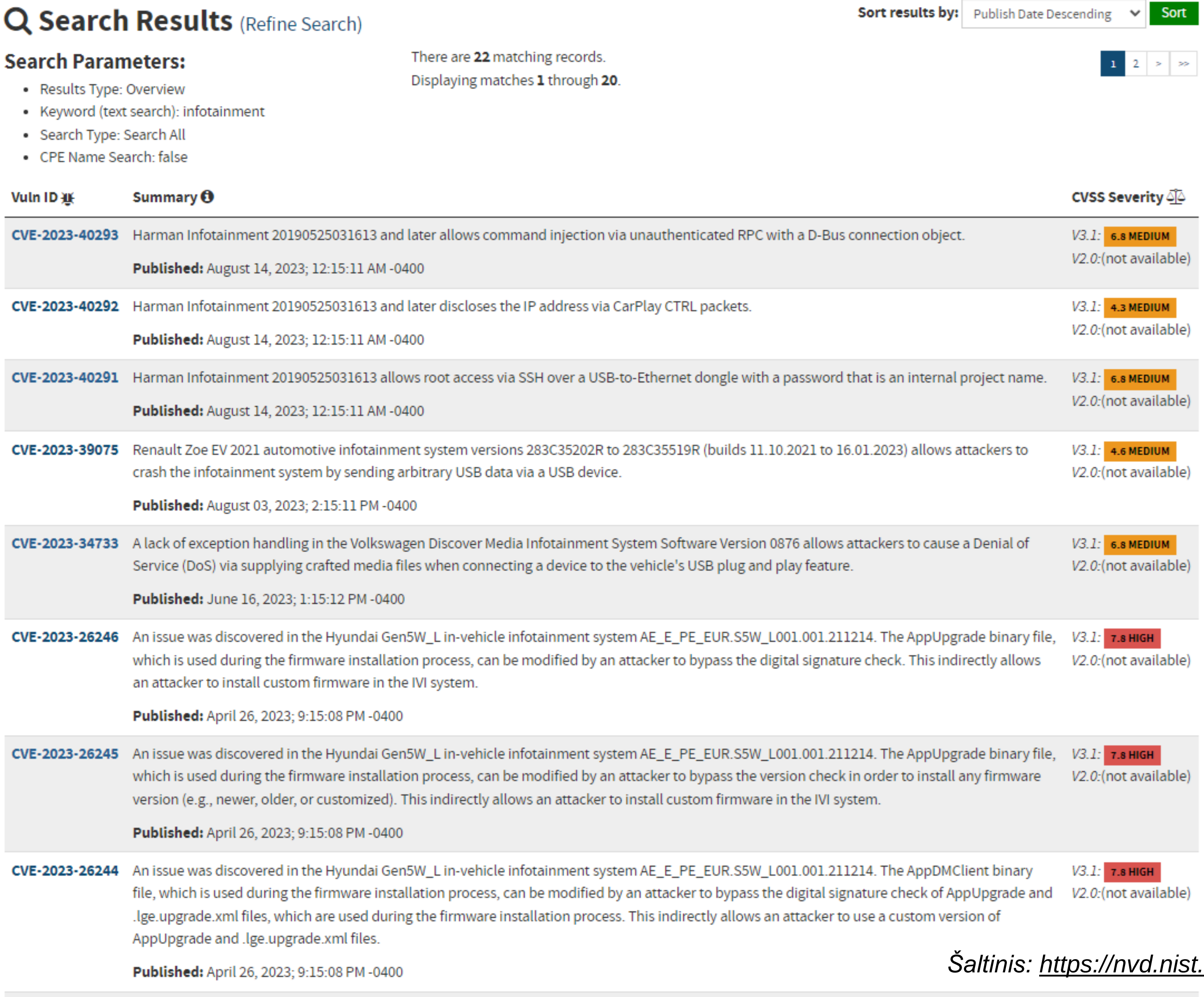
Kaip: CVE-2015-5611

Pasekmės: Atšaukti 1.4 milijonai vienetų.

- 2013-2015 MY Dodge Viper specialty vehicles
- 2013-2015 Ram 1500, 2500 and 3500 pickups
- 2013-2015 Ram 3500, 4500, 5500 Chassis Cabs
- 2014-2015 Jeep Grand Cherokee and Cherokee SUVs
- 2014-2015 Dodge Durango SUVs
- 2015 MY Chrysler 200, Chrysler 300 and Dodge Charger sedans
- 2015 Dodge Challenger sports coupes



The Jeep Cherokee is the only vehicle to be recalled due to its potential hackability, with 1.4 million cars (various Dodge, Jeep, and Chrysler models) being voluntarily recalled in response to research finding that they were vulnerable. The company claims that there had been no known injuries related to hacking of vehicle systems.



Search Results (Refine Search)

Sort results by: Publish Date Descending | Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): infotainment
- Search Type: Search All
- CPE Name Search: false

There are **22** matching records.
Displaying matches **1** through **20**.

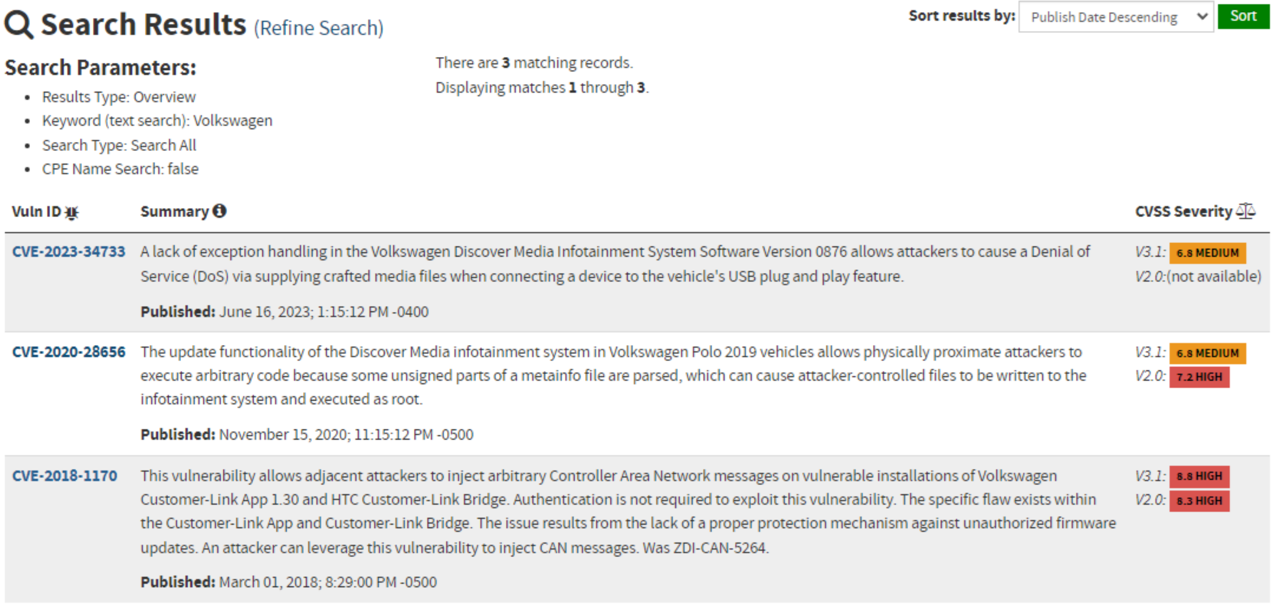
1 2 > >>

Vuln ID	Summary	CVSS Severity
CVE-2023-40293	Harman Infotainment 20190525031613 and later allows command injection via unauthenticated RPC with a D-Bus connection object. **Published:** August 14, 2023; 12:15:11 AM -0400	*V3.1:* 6.8 MEDIUM *V2.0:*(not available)
CVE-2023-40292	Harman Infotainment 20190525031613 and later discloses the IP address via CarPlay CTRL packets. **Published:** August 14, 2023; 12:15:11 AM -0400	*V3.1:* 4.3 MEDIUM *V2.0:*(not available)
CVE-2023-40291	Harman Infotainment 20190525031613 allows root access via SSH over a USB-to-Ethernet dongle with a password that is an internal project name. **Published:** August 14, 2023; 12:15:11 AM -0400	*V3.1:* 6.8 MEDIUM *V2.0:*(not available)
CVE-2023-39075	Renault Zoe EV 2021 automotive infotainment system versions 283C35202R to 283C35519R (builds 11.10.2021 to 16.01.2023) allows attackers to crash the infotainment system by sending arbitrary USB data via a USB device. **Published:** August 03, 2023; 2:15:11 PM -0400	*V3.1:* 4.6 MEDIUM *V2.0:*(not available)
CVE-2023-34733	A lack of exception handling in the Volkswagen Discover Media Infotainment System Software Version 0876 allows attackers to cause a Denial of Service (DoS) via supplying crafted media files when connecting a device to the vehicle's USB plug and play feature. **Published:** June 16, 2023; 1:15:12 PM -0400	*V3.1:* 6.8 MEDIUM *V2.0:*(not available)
CVE-2023-26246	An issue was discovered in the Hyundai Gen5W_L in-vehicle infotainment system AE_E_PE_EUR.S5W_L001.001.211214. The AppUpgrade binary file, which is used during the firmware installation process, can be modified by an attacker to bypass the digital signature check. This indirectly allows an attacker to install custom firmware in the IVI system. **Published:** April 26, 2023; 9:15:08 PM -0400	*V3.1:* 7.8 HIGH *V2.0:*(not available)
CVE-2023-26245	An issue was discovered in the Hyundai Gen5W_L in-vehicle infotainment system AE_E_PE_EUR.S5W_L001.001.211214. The AppUpgrade binary file, which is used during the firmware installation process, can be modified by an attacker to bypass the version check in order to install any firmware version (e.g., newer, older, or customized). This indirectly allows an attacker to install custom firmware in the IVI system. **Published:** April 26, 2023; 9:15:08 PM -0400	*V3.1:* 7.8 HIGH *V2.0:*(not available)
CVE-2023-26244	An issue was discovered in the Hyundai Gen5W_L in-vehicle infotainment system AE_E_PE_EUR.S5W_L001.001.211214. The AppDMClient binary file, which is used during the firmware installation process, can be modified by an attacker to bypass the digital signature check of AppUpgrade and .lge.upgrade.xml files, which are used during the firmware installation process. This indirectly allows an attacker to use a custom version of AppUpgrade and .lge.upgrade.xml files. **Published:** April 26, 2023; 9:15:08 PM -0400	*V3.1:* 7.8 HIGH *V2.0:*(not available)

Šaltinis: https://nvd.nist.gov/vuln/search

Kokio modelio lengvųjų automobilių Lietuvoje yra daugiausia?

„Volkswagen Passat“ – toks atsakymas į pavadinime užduotą klausimą. Lietuvoje 2022 m. sausio 1 d. buvo registruoti 89 477 „Volkswagen Passat“ automobiliai. Tai reiškia, kad „Volkswagen Passat“ vairuoja kas trisdešimtas Lietuvos gyventojas.



Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): Volkswagen
- Search Type: Search All
- CPE Name Search: false

There are **3** matching records.
Displaying matches **1** through **3**.

Vuln ID	Summary	CVSS Severity
CVE-2023-34733	A lack of exception handling in the Volkswagen Discover Media Infotainment System Software Version 0876 allows attackers to cause a Denial of Service (DoS) via supplying crafted media files when connecting a device to the vehicle's USB plug and play feature. **Published:** June 16, 2023; 1:15:12 PM -0400	*V3.1:* 6.8 MEDIUM *V2.0:*(not available)
CVE-2020-28656	The update functionality of the Discover Media infotainment system in Volkswagen Polo 2019 vehicles allows physically proximate attackers to execute arbitrary code because some unsigned parts of a metainfo file are parsed, which can cause attacker-controlled files to be written to the infotainment system and executed as root. **Published:** November 15, 2020; 11:15:12 PM -0500	*V3.1:* 6.8 MEDIUM *V2.0:* 7.2 HIGH
CVE-2018-1170	This vulnerability allows adjacent attackers to inject arbitrary Controller Area Network messages on vulnerable installations of Volkswagen Customer-Link App 1.30 and HTC Customer-Link Bridge. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Customer-Link App and Customer-Link Bridge. The issue results from the lack of a proper protection mechanism against unauthorized firmware updates. An attacker can leverage this vulnerability to inject CAN messages. Was ZDI-CAN-5264. **Published:** March 01, 2018; 8:29:00 PM -0500	*V3.1:* 8.8 HIGH *V2.0:* 8.3 HIGH

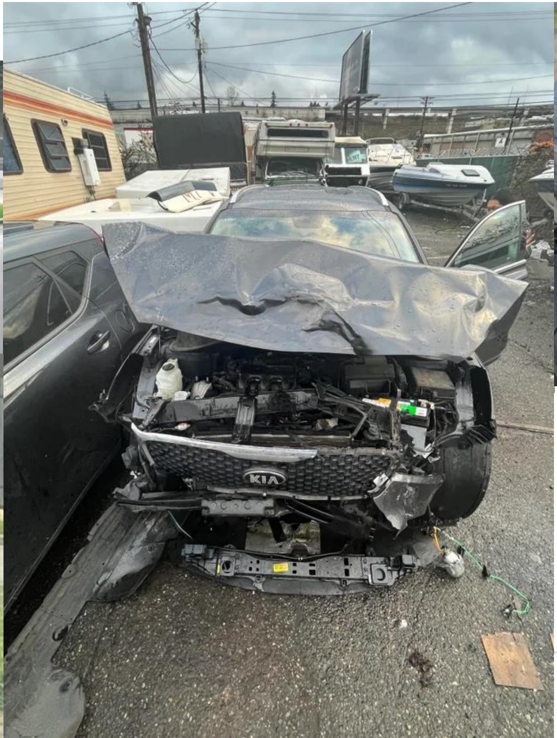
Tai ar lengva visgi įsilaužti į automobilį?

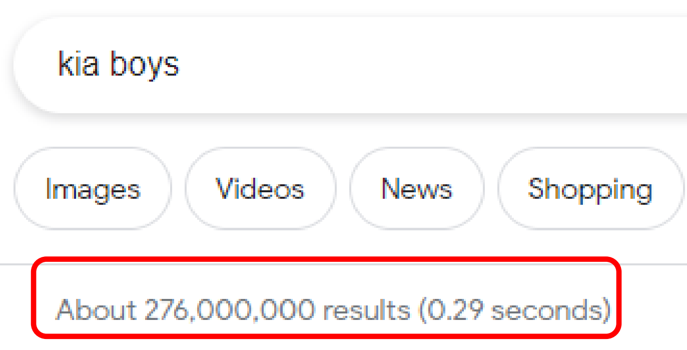
Ir taip, ir ne…

Kia ir Hyundai incidentas

Kia ir Hyundai incidentas

Kia Boys tendencija



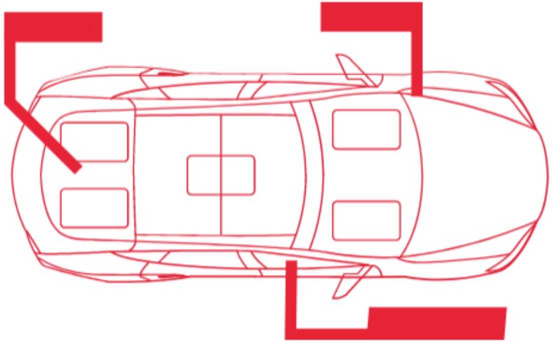


kia boys

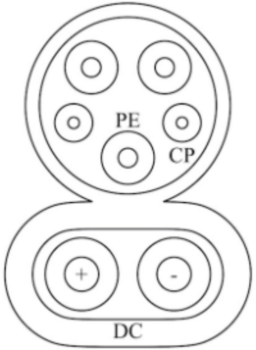
About 276,000,000 results (0.29 seconds)

Flipper zero

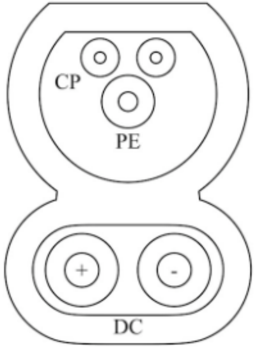
Ar taikinys tik automobiliai?



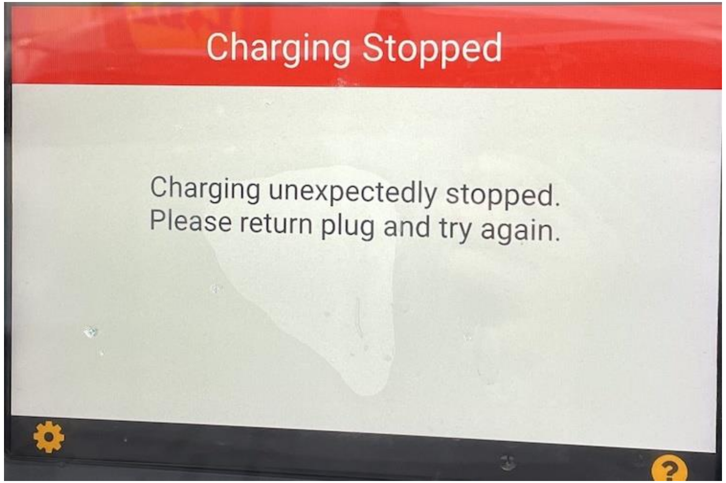
Brokenwire ataka



(a) CCS Combo 1 (US).



(b) CCS Combo 2 (EU).



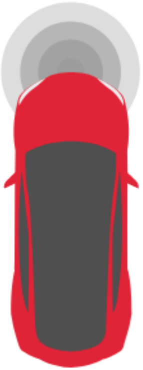
Charging Stopped

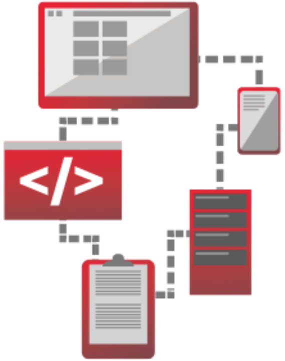
Charging unexpectedly stopped.
Please return plug and try again.

LimeSDR

Šaltinis: https://www.brokenwire.fail/

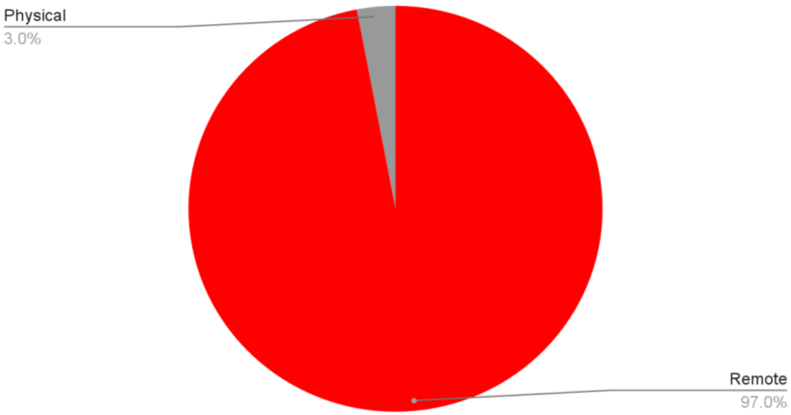
Ar būtina turėti automobilį ?



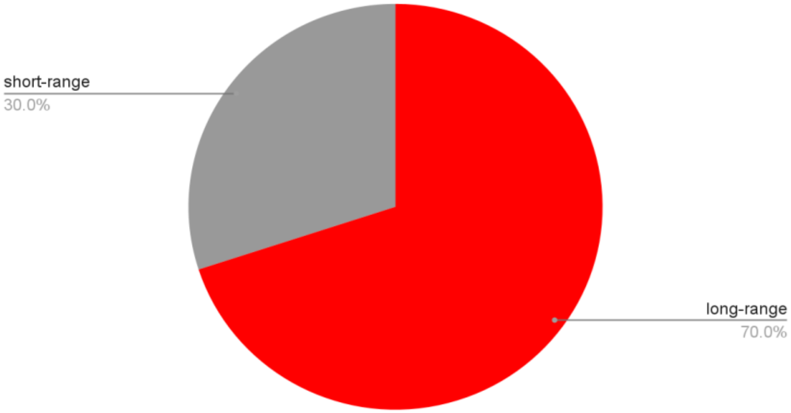


Long-range attacks increased in 2022 due to increased connectivity and API reliance

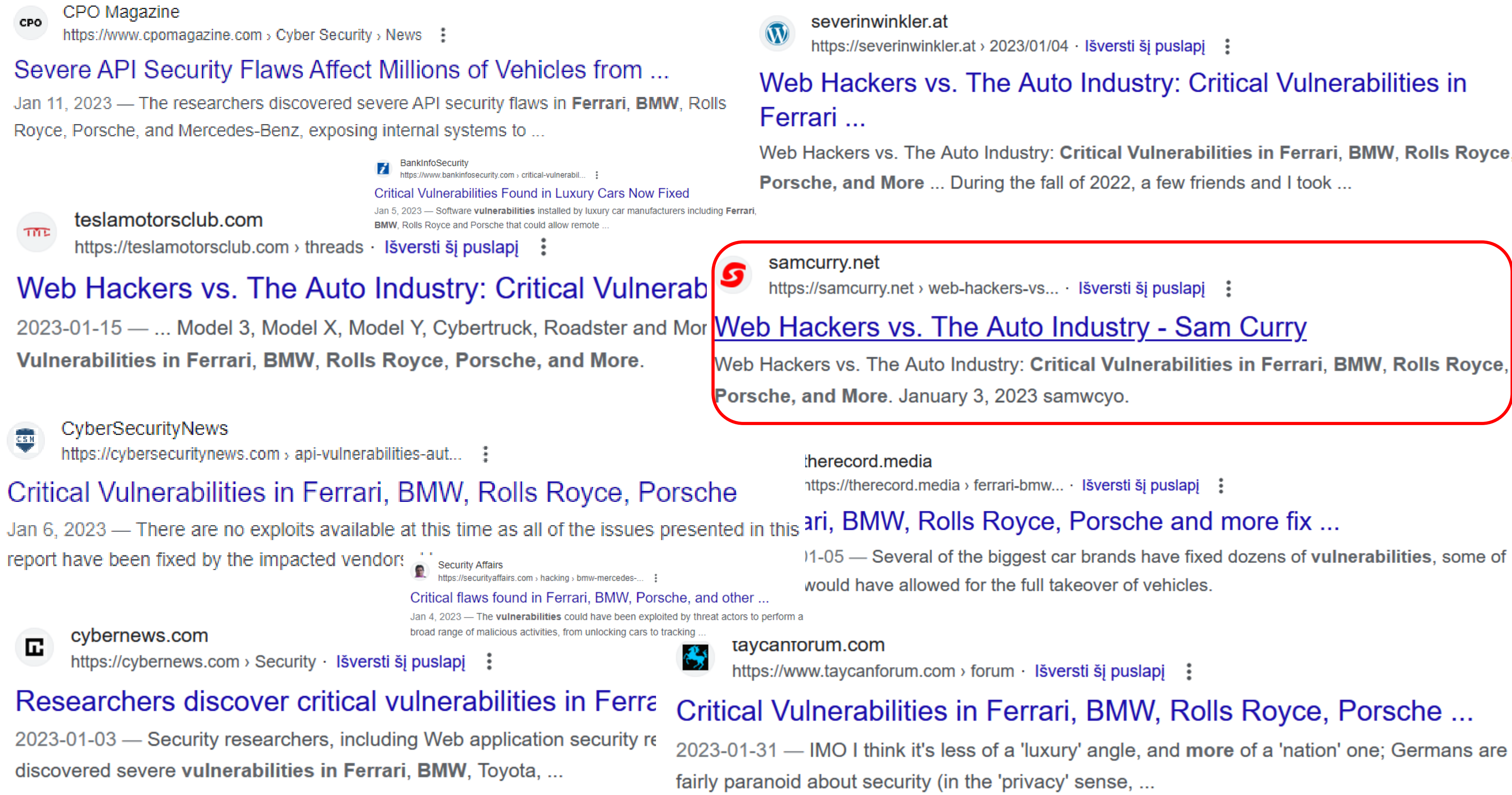
Nearly all 2022 attacks are remote



Over two thirds of 2022 remote attacks were long-range



Šaltinis: Upstream 2023 Global Automotive Cybersecurity Report



CPO Magazine
https://www.cpomagazine.com › Cyber Security › News

Severe API Security Flaws Affect Millions of Vehicles from ...

Jan 11, 2023 — The researchers discovered severe API security flaws in **Ferrari**, **BMW**, Rolls Royce, Porsche, and Mercedes-Benz, exposing internal systems to ...

BankInfoSecurity
https://www.bankinfosecurity.com › critical-vulnerabil...

Critical Vulnerabilities Found in Luxury Cars Now Fixed

Jan 5, 2023 — Software **vulnerabilities** installed by luxury car manufacturers including **Ferrari**, **BMW**, Rolls Royce and Porsche that could allow remote ...

teslamotorsclub.com
https://teslamotorsclub.com › threads · Išversti šį puslapį

Web Hackers vs. The Auto Industry: Critical Vulnerab

2023-01-15 — ... Model 3, Model X, Model Y, Cybertruck, Roadster and Mor

Vulnerabilities in Ferrari, **BMW**, **Rolls Royce**, **Porsche**, **and More**.

CyberSecurityNews
https://cybersecuritynews.com › api-vulnerabilities-aut...

Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche

Jan 6, 2023 — There are no exploits available at this time as all of the issues presented in this report have been fixed by the impacted vendors

Security Affairs
https://securityaffairs.com › hacking › bmw-mercedes-...

Critical flaws found in Ferrari, BMW, Porsche, and other ...

Jan 4, 2023 — The **vulnerabilities** could have been exploited by threat actors to perform a broad range of malicious activities, from unlocking cars to tracking ...

cybernews.com
https://cybernews.com › Security · Išversti šį puslapį

Researchers discover critical vulnerabilities in Ferra

2023-01-03 — Security researchers, including Web application security re discovered severe **vulnerabilities in Ferrari**, **BMW**, Toyota, ...

severinwinkler.at
https://severinwinkler.at › 2023/01/04 · Išversti šį puslapį

Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari ...

Web Hackers vs. The Auto Industry: **Critical Vulnerabilities in Ferrari**, **BMW**, **Rolls Royce**, **Porsche**, **and More** ... During the fall of 2022, a few friends and I took ...

samcurry.net
https://samcurry.net › web-hackers-vs... · Išversti šį puslapį

Web Hackers vs. The Auto Industry - Sam Curry

Web Hackers vs. The Auto Industry: **Critical Vulnerabilities in Ferrari**, **BMW**, **Rolls Royce**, **Porsche**, **and More**. January 3, 2023 samwcyo.

therecord.media
https://therecord.media › ferrari-bmw... · Išversti šį puslapį

ari, BMW, Rolls Royce, Porsche and more fix ...

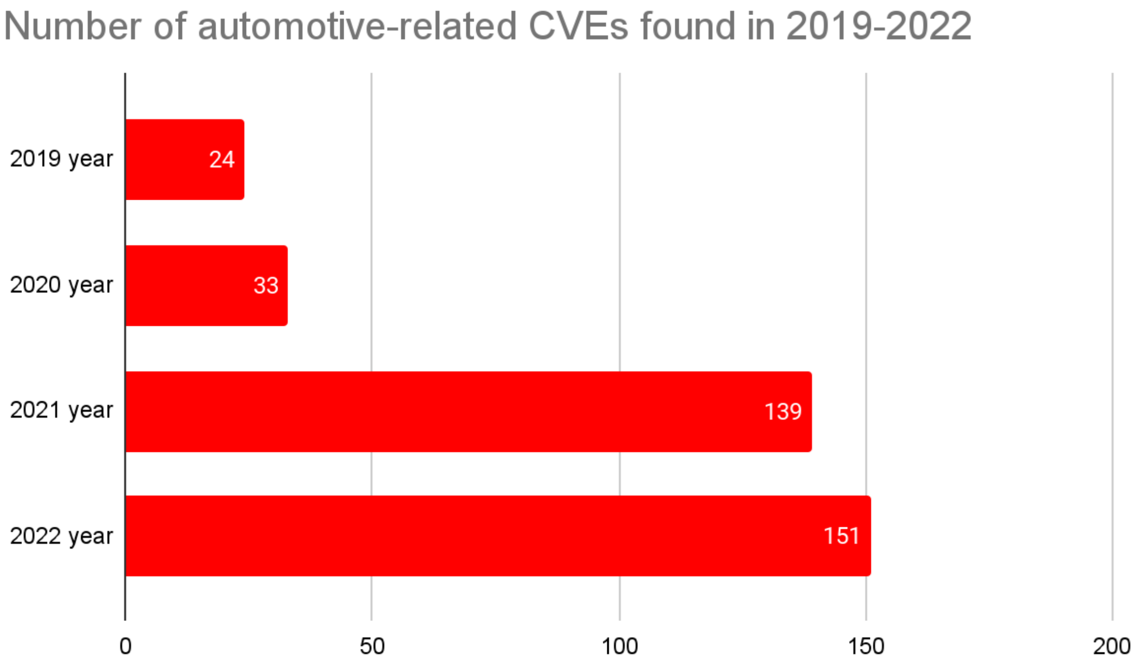
1-05 — Several of the biggest car brands have fixed dozens of **vulnerabilities**, some of would have allowed for the full takeover of vehicles.

taycanforum.com
https://www.taycanforum.com › forum · Išversti šį puslapį

Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche ...

2023-01-31 — IMO I think it's less of a 'luxury' angle, and **more** of a 'nation' one; Germans are fairly paranoid about security (in the 'privacy' sense, ...

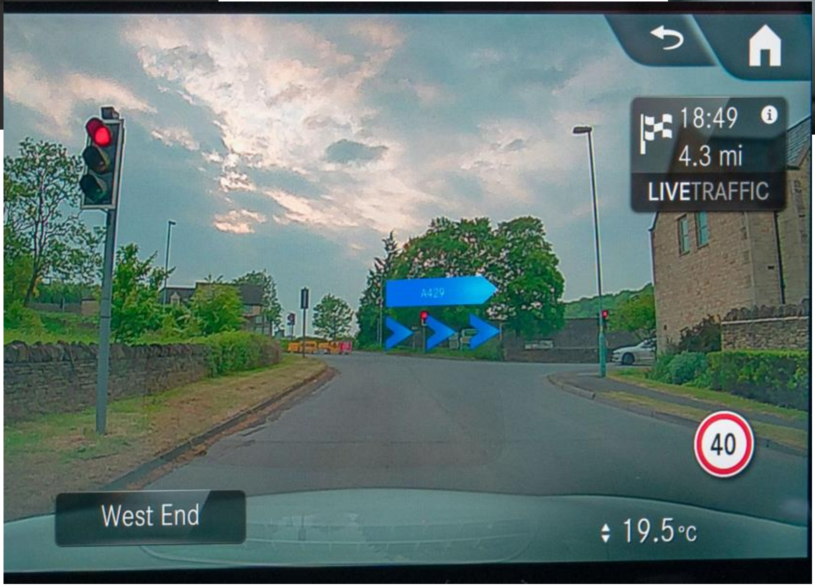
Kokia visgi ateitis laukia?



Šaltinis: Upstream 2023 Global Automotive Cybersecurity Report

Nauji funkcionalumai - patogumas ar grėsmė?

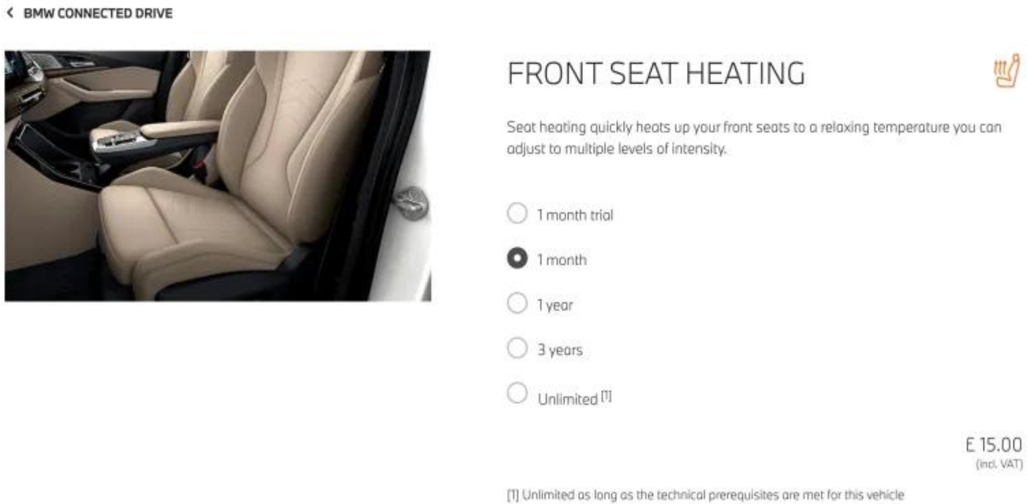
Mitsubishi signaling system



Mercedes Benz augmented reality navigation

Audi e-Tron virtual mirrors

Prenumeratos



‹ BMW CONNECTED DRIVE

FRONT SEAT HEATING

Seat heating quickly heats up your front seats to a relaxing temperature you can adjust to multiple levels of intensity.

○ 1 month trial

● 1 month

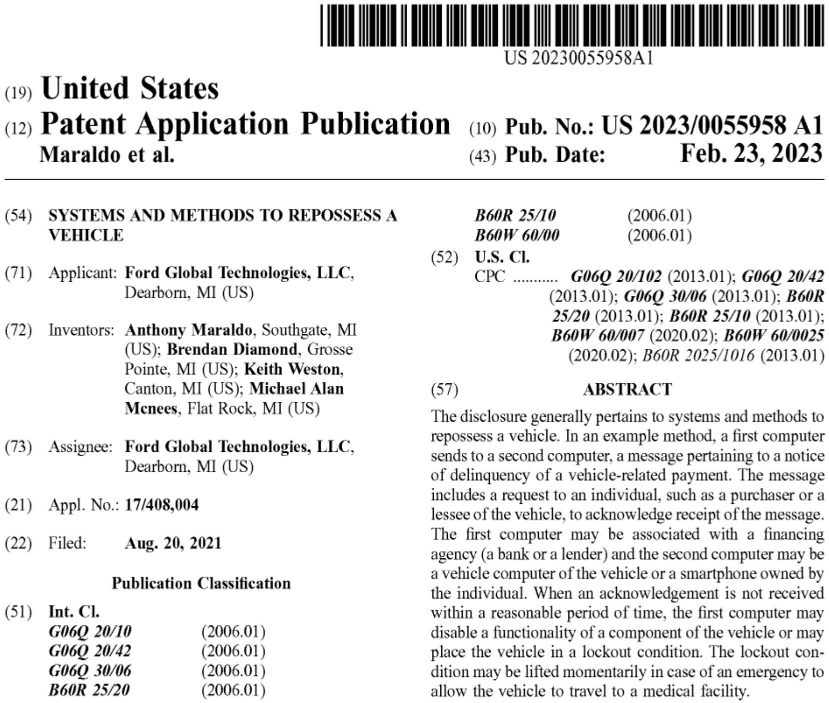
○ 1 year

○ 3 years

○ Unlimited [1]

£ 15.00
(incl. VAT)

[1] Unlimited as long as the technical prerequisites are met for this vehicle



US 20230055958A1

(19) **United States**

(12) **Patent Application Publication**
Maraldo et al.

(10) **Pub. No.: US 2023/0055958 A1**

(43) **Pub. Date: Feb. 23, 2023**

(54) **SYSTEMS AND METHODS TO REPOSSESS A VEHICLE**

(71) Applicant: **Ford Global Technologies, LLC**, Dearborn, MI (US)

(72) Inventors: **Anthony Maraldo**, Southgate, MI (US); **Brendan Diamond**, Grosse Pointe, MI (US); **Keith Weston**, Canton, MI (US); **Michael Alan Mcnees**, Flat Rock, MI (US)

(73) Assignee: **Ford Global Technologies, LLC**, Dearborn, MI (US)

(21) Appl. No.: **17/408,004**

(22) Filed: **Aug. 20, 2021**

Publication Classification

(51) **Int. Cl.**

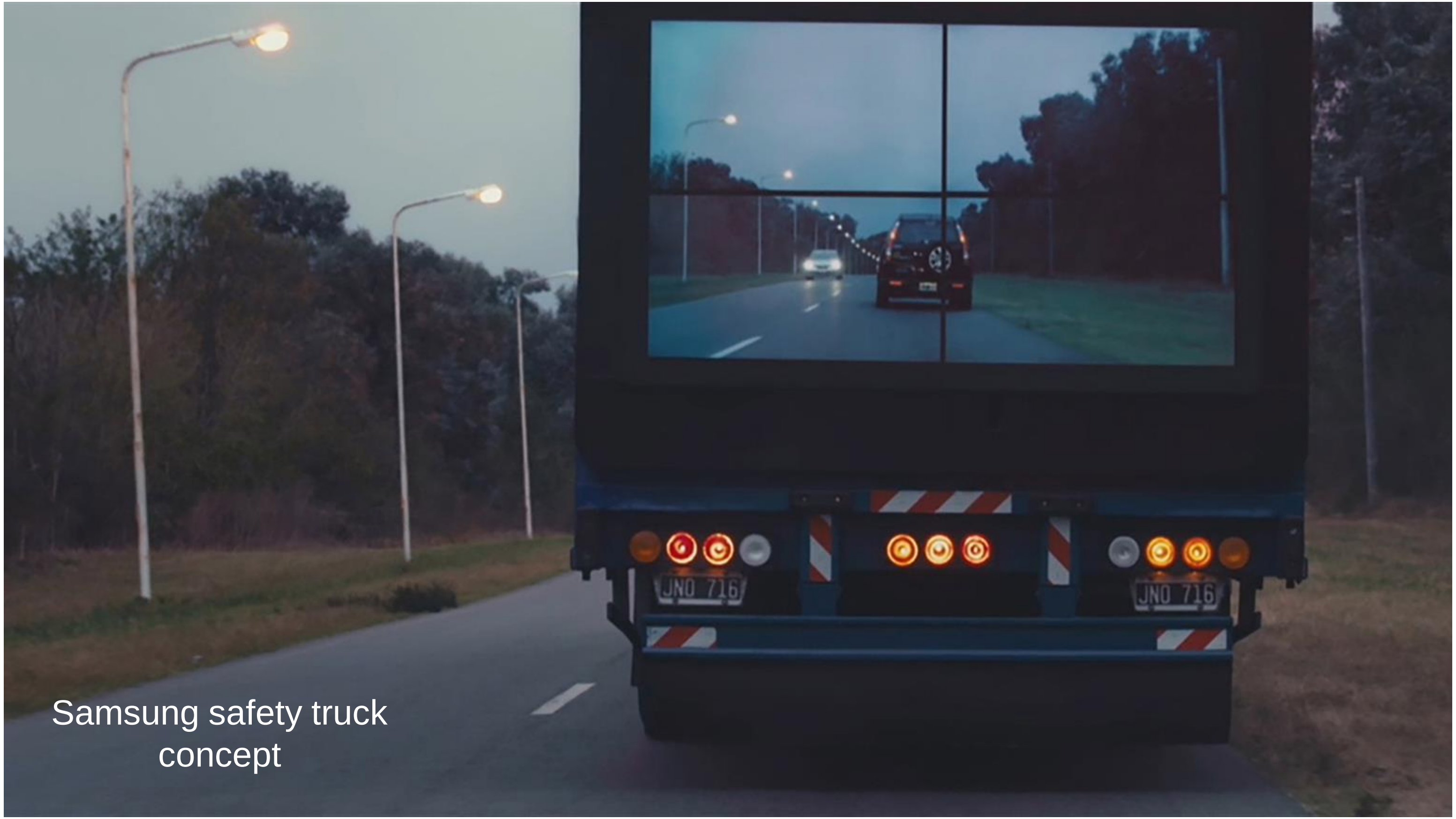
G06Q 20/10	(2006.01)
G06Q 20/42	(2006.01)
G06Q 30/06	(2006.01)
B60R 25/20	(2006.01)
B60R 25/10	(2006.01)
B60W 60/00	(2006.01)

(52) **U.S. Cl.**
CPC ***G06Q 20/102*** (2013.01); ***G06Q 20/42*** (2013.01); ***G06Q 30/06*** (2013.01); ***B60R 25/20*** (2013.01); ***B60R 25/10*** (2013.01); ***B60W 60/007*** (2020.02); ***B60W 60/0025*** (2020.02); *B60R 2025/1016* (2013.01)

(57) **ABSTRACT**

The disclosure generally pertains to systems and methods to repossess a vehicle. In an example method, a first computer sends to a second computer, a message pertaining to a notice of delinquency of a vehicle-related payment. The message includes a request to an individual, such as a purchaser or a lessee of the vehicle, to acknowledge receipt of the message. The first computer may be associated with a financing agency (a bank or a lender) and the second computer may be a vehicle computer of the vehicle or a smartphone owned by the individual. When an acknowledgement is not received within a reasonable period of time, the first computer may disable a functionality of a component of the vehicle or may place the vehicle in a lockout condition. The lockout condition may be lifted momentarily in case of an emergency to allow the vehicle to travel to a medical facility.

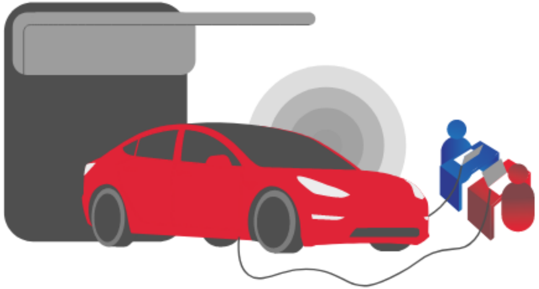
Without security there is no safety



Samsung safety truck concept

Kaip apsaugoti?

- Faradėjaus dėklas
- Atnaujinti programinę įrangą
- Jei kraunate, patikrinkite progresą
- Jei naudojate aplikaciją ar turite paskyrą, apsaugokite stipriu slaptažodžiu
- Išjunkite nenaudojamus funkcionalumus kaip, pavyzdžiui, Bluetooth
- Naudoti patikimą įrangą
- Sekimo prietaisas



ASRG

LITHUANIA

https://www.meetup.com/automotive-security-research-group-lithuania/

Ačiū už dėmesį