CYBELLUM

The State of Automotive Security in 2023:

Implementing a secure future

Table of Contents

The data *doesn't lie*

The data uncovered in this year's report reflects a trend that we've been tracking for some time across the automotive industry. The best way to describe it is a new optimism, blended with an ever-present caution of what the future holds.

While there's much to say surrounding the future of vehicles, the old adage of "If it isn't broken, don't fix it" won't work for the automotive sector– and the ecosystem knows it.

In response, we found that organizations are starting to work as teams to obtain a more mature product security posture. Product security professionals are taking it upon themselves to conduct their product security tasks with a sense of urgency. The data below, all based on Cybellum's private database, reflects these changes and a stronger foundation for more secure vehicles to begin rolling off production lines.

However, while we eagerly await the day of robustly secured vehicles, we are not there yet. The reliance on high-risk OSS components, along with the uncomfortable frequency of popular CVEs that still reside in many of our embedded components means that the cybersecurity community must continue raising red flags.

With the full implementation of WP.29 R155 coming into effect on July 1, 2024, it's the 11th hour for companies to take a hard look at their software development and vulnerability management processes. With so many CVEs, outdated software components, and old vulnerabilities being introduced into vehicles, it's time for executives through product security practitioners practitioners to roll up their sleeves and double down on automation to meet CSMS requirements.

Special thanks to our Cybersecurity Analyst team for compiling the internal data that this report is built upon.

- Rafi Spiewak, Director of Content

Key takeaways and methodology

In 2023, the data is mixed but the story is clear. While companies continue to push towards meeting newly-implemented standards and regulations via the implementation of automation and Cybersecurity management systems (CSMS), they are struggling to understand the true risk in their existing components.

The information in this report is based on our vast internal resources which includes vehicles on the road today as well as those in production.

1

Old threats remain persistent - Despite the greater awareness surrounding secure development, vulnerabilities are making their way into devices at a significantly faster rate than ever before. Without automation and streamlined vulnerability management and prioritization, this number seems poised to grow exponentially.

2

Security is playing a bigger role - We have seen an increase in operating systems that have inherent security capabilities built in. While developers continue to rely on Android, which is found in 22% of components, up from 18% In 2022, more are turning to another proven OS, Debian, which is used 18.1% of the time compared to just 4.1% last year.

3

Fewer private keys are being detected - There appears to be a growing awareness amongst developers and product security practitioners. This step reduces risk to the components, should their private key become exposed (see more on page 10).

4

Developers are stuck in a 'if it isn't broken, don't fix it' mindset - The data shows reason to believe that newer software is developed securely. However, existing components that have known vulnerabilities keep finding their way into new vehicles. This is apparent through the continued presence of end of life (EOL), end of service (EOS), and no longer maintained software – introducing old risks into new vehicles.

Where we are: The state of automotive cybersecurity

While there has no doubt been great progress in the world of automotive product security, there is still a way to go in terms of maturity.

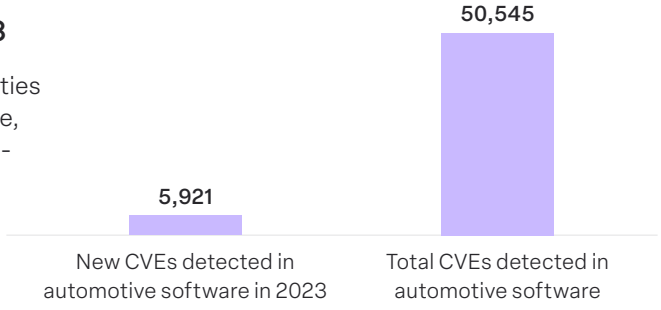
The data tells a complicated story of critical vulnerabilities that seem to stubbornly find their way into new vehicles. OEMs and suppliers who sell throughout Europe and beyond will soon have to answer to governments and shareholders for the known risks they have neglectfully allowed in the software supply chain.

Vulnerability relevancy is dropping

The high frequency of vulnerabilities and weaknesses are an unfortunate reality for many connected products across sectors, including the automotive industry.
We are seeing more CVEs associated with software used in vehicles, but upon further analysis, we find that only a small fraction are actually relevant or potentially-exploitable in the specific context of the product.
In fact, we see a slight decrease in the number of relevant CVEs YoY despite a jump from 2022 to 2023.

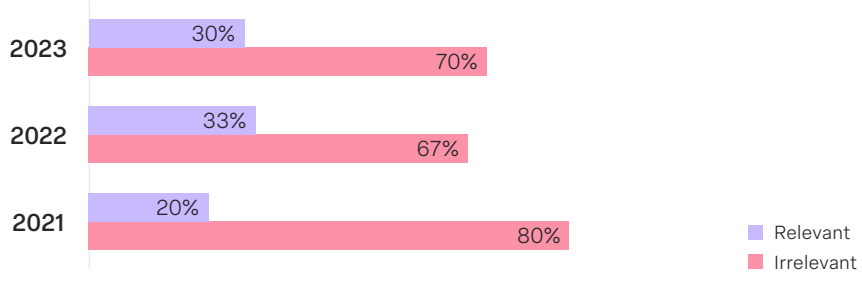
Vulnerabilities jumped in 2023

A significant percentage of vulnerabilities have been discovered in this year alone, accounting for 11% of total automotive-related CVEs.



Those without automation will be forced to increase their workforce, assigning more people in finding each 'needle in a haystack' vulnerability, costing time and resources that should be spent on addressing high-priority risks.

Relevant vs. Irrelevant vulnerabilities



Relevant vulnerabilities are down to 30%, compared to 33% in 2022, but still above 2021's 20%
The implementation of product security automation and vulnerability management & prioritization prioritization, such what the VM co-pilot addresses, is helping teams identify where to focus resources.

However, being able to obtain the visibility needed to ensure they don't find their way into a product calls for a centralized dashboard where product security teams can keep a vehicle secure from vulnerabilities that have emerged well after it drives off the lot.

To achieve compliance with R155 and ISO/SAE21434, product security teams are going to need to remain proactive as they scale their activities. The first step to this is aligning security activities across departments as a means to gain unprecedented visibility into their vehicles.

Old threats and challenges remain

While the pace of new software development continues to increase with the help of AI, many of the software components present in vehicles across the industry (over 1 in 5) are older than 10 years.

Components that were developed 10+ years ago were developed in a time of a very different product security landscape than vehicles face today. Yet, just as in 2022, 24% of all components are still a decade or more old, introducing a great variation between the product security standards of components today and the older ones that they operate along side.

Using end of life or end of service software component packages kicks the can down the road, compounding the cybersecurity problems that will likely arise later. As new and old vulnerabilities are discovered within products, it is worthwhile for teams to identify these outdated components and consider swapping them for more secure options.

Most common packages that are over a decade old

zlib1.2.8	dnsmasq2.51
bzip21.0.6*	cracklib2.9.0
zlib1.2.3	alsa_lib1.0.27.2
libexif0.6.21	commons_logging1.1.0
libcap2.22*	alsa_utils1.0.27.2
httpcomponents_client4.0	expat2.1.0
jsip1.2.169	ppp2.4.5
iputils20121221	

* Has multiple CVEs with varying severities

CVEs for OSS components are common in vehicles

While developers speed up development using open source components, they also rely on libraries maintained and created by a trusted community of their peers. When it comes to security, their ability to conduct thorough security testing is the difference between a secure device and one that poses a danger to operators.

However, 2023 data shows that many of the most notorious CVEs, many with a CVSS v3 score of 10.0, are still embedded in vehicles today.

This unacceptable level of risk speaks to the wide gap across the automotive industry regarding how vulnerabilities are discovered, shared, and addressed. Soon, with the implementation of WP.29 R155, R156, and ISO/SAE 21434, companies will have to implement some standardized practices regarding automotive cybersecurity vulnerabilities. This can harbor a greater discussion of not only how to minimize vulnerabilities but prevent them from ever entering the software supply chain.

Most notorious CVEs still embedded in vehicles

Nickname	CVE #	CVSS V3 Score
BleedingTooth	CVE-2020-12352	High, 8.8
BleedingTooth	CVE-2020-12351	High, 7.5
Sweet32	CVE-2016-2183	High, 8.0
BleedingTooth	CVE-2020-24490	Medium, 5.9
BlueBorne	CVE-2017-1000250	Medium, 6.5
Spectre	CVE-2017-5715	High, 7.8
Spectre	CVE-2017-5753	Critical, 10.0 Based on CVSS v2.0
Drown	CVE-2016-0800	Critical 10.0
DirtyCow	CVE-2016-5195	High, 7.5
BlueBorne	CVE-2017-1000251	High, 7.5
Heartbleed	CVE-2014-0160	High, 7.6

CWEs

Common Weakness Enumeration (CWEs) are a simplified report to classify security weaknesses within physical or software-driven systems.

> ***CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.***
>
> cwe.mitre.org

Similar to CVEs, CWEs are named using a numerical system so they can be easily recalled and updated as needed. Unlike a specific attack, these common weaknesses may include tricking a system into sharing personal information, forcing it to shut down, or another unauthorized function.

While the automotive industry is praised for best understanding the market's needs, the use of obsolete functions (1.4% of top CWEs in 2023), while relatively low, is still a cause for alarm, and buffer overflows (2.2% of top CWEs in 2023), which have the potential to completely disable a device, is still relatively common.

Top CWEs in 2023

In 2023, 87% of weaknesses surrounded exposing sensitive information. However, other less-common CWEs still hold great risk for a high-impact event, such as stack overflow.

CWE #(s)	Error	Total percentage of CWEs
CWE-209,CWE-215	Generation of Error Message Containing Sensitive Information	69%
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	18%
CWE-476,CWE-690	NULL Pointer Dereference, Unchecked Return Value to Value to NULL Pointer Dereference	2.1%
CWE-121	Stack-based Buffer Overflow	2.1%
CWE-76,CWE-77,CWE-78	Improper Neutralization of Equivalent Special Elements	1.6%
CWE-477	Use of Obsolete Function	1.4%
CWE-120,CWE-124,CWE-126, CWE-127,CWE-242	Buffer Copy without Checking Size of Input	1.3%
CWE-835	Loop with Unreachable Exit Condition	1.2%
CWE-1120	Excessive Code Complexity	1.0%
CWE-674	Uncontrolled Recursion	0.7%
CWE-252	Unchecked Return Value	0.6%
CWE-416	Use After Free	0.6%

Unnecessary risk

Much of the vulnerabilities we are seeing throughout connected automotive components continue to remain those whose true risk posture was exposed years ago. By not identifying all embedded software components, teams are unable to identify if any are outdated, have reached end of service (EOS), or end of life (EOL). When software is not maintained, there is no way to know that it is unserviceable without conducting a full product security check– even within the AUTOSAR or other frameworks.

Relying on older components potentially exposing vehicles to exploits found in the wild.

As development teams continue to build upon old functionality to develop new features, common vulnerabilities continue to find their way into today's products via EOS/EOL software or outdated versions of current components among others.

Most commonly used packages over 10 years old

Those with an asterisk have appeared on this list in prior years as well.

zlib*	libpng*
openssl*	boost
gcc*	qt
sqlite	ncurses*
android_framework_native	curl

Most notorious CVEs still found in automotive technologies in order of frequency and with criticality

vuln_id	Package	Severity
CVE-2018-25032	Zlib	High
CVE-2022-37434	Zlib	Critical
CVE-2023-45853	Zlib	Critical
CVE-2023-4039	gcc	Medium
CVE-2023-3446	OpenSSL	Medium
CVE-2023-3817	OpenSSL	Medium
CVE-2023-0465	OpenSSL	Medium
CVE-2023-0215	OpenSSL	High
CVE-2021-37322	gcc	High
CVE-2023-0286	OpenSSL	High
CVE-2023-2650	OpenSSL	Medium
CVE-2023-0464	OpenSSL	High

OS security and software supply chain risk

2023 has seen a shift from 2022 in regards to the use of more secure operating systems, ones that are more stable and can protect the components within from being breached.

With the increased cadence of new automotive code, it will be critical for OEMs to implement regulations surrounding robust software supply chain security measures. With an eye on CASE vehicles in the near future, the automotive industry is responsible not only for safeguarding against potential cyber threats but also for maintaining the overall integrity and safety of connected vehicles. This includes relying on a secure OS to execute the software.

Top operating systems used in 2023

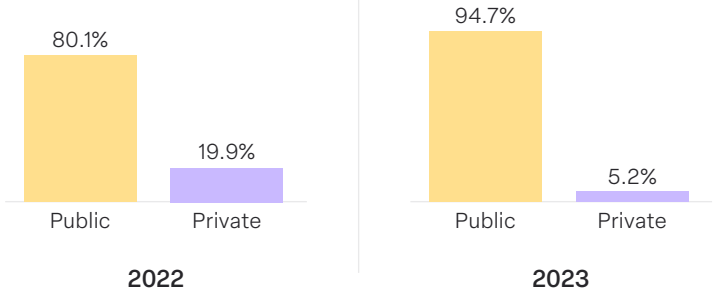
OS name	Frequency	Frequency in 2022
Android	21.9%	16.3%
Debian	18.8%	4.1%
Autosar Classic	9.4%	4.1%
QNX	9.4%	10.2%
Arago	6.3%	NA
Freescale i.mx	6.3%	NA
Windows	12.6%	16.3%
yocto_genivi_baseline	6.3%	NA
Linux	3.1%	14.3%

Encryption keys

One trend that the data exposes is the reduction of exposed private keys in automotive firmware, dropping down to just over 5% in 2023 from nearly 20% in 2022.

The continued year over year trend of fewer detected private keys may represent a growing awareness by engineering and product security teams to the sensitivity of private keys.

Public vs. Private encryption keys in 2022 vs. 2023



Future focused

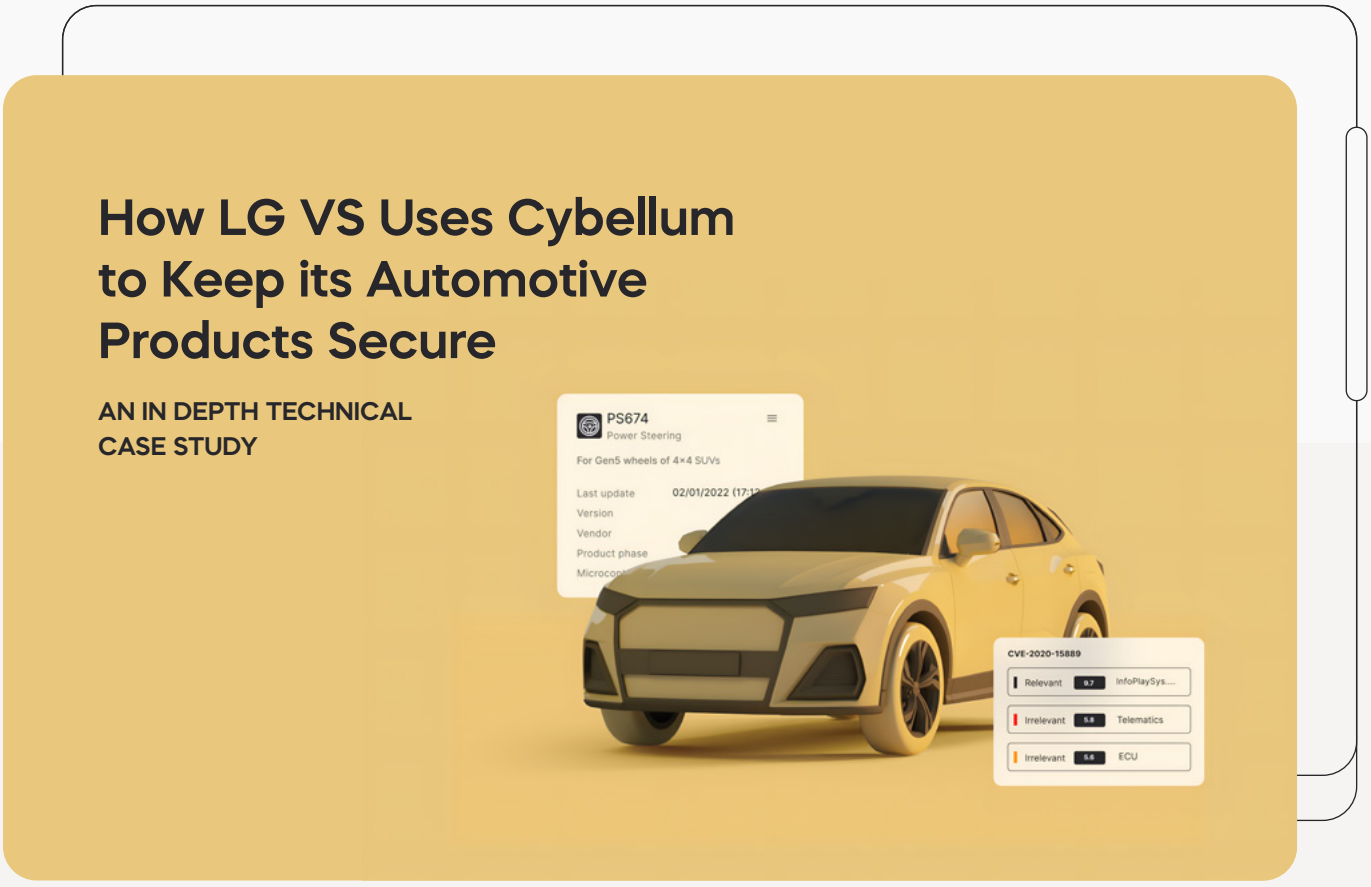
Despite the current state of automotive software security, there is reason to be hopeful for a more secure future.

As WP.29 R155, R156, and ISO/SAE 21434 approach and pass their enforcement dates, many of the changes we are seeing are a step towards greater compliance. More companies are working to identify their vulnerabilities, mitigate them, and ensure security well after vehicles roll off the assembly line.

There is no doubt that there is no longer room for the introduction of old risks into new vehicles. Relying on old embedded software components and old operating systems will only continue to bring those same old problems into a future that will rely on their security posture like never before.

It's no surprise to anyone in the ecosystem that vulnerability management is necessary. Yet, the lack of properly addressing vulnerabilities will lead to compliance issues, and potentially market and financial losses.

Solutions like the CSMS Cockpit, developed by Cybellum and LG Vehicle Component Solutions, help automate and facilitate the CSMS process from start to finish.



Cybellum Helped LG Vehicle Component Services achieve CSMS certification and improve component visibility

About us

CYBELLUM IS WHERE TEAMS DO PRODUCT SECURITY.

Top Automotive manufacturers such as Jaguar Land Rover, Nissan, Audi, and Faurecia use Cybellum's Product Security Platform and services to manage the main aspects of their cybersecurity operations across business units and lifecycle stages. From SBOM to Vulnerability Management, Compliance Validation, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

Experience what product security can be. Book a demo.

Learn more about Product Security

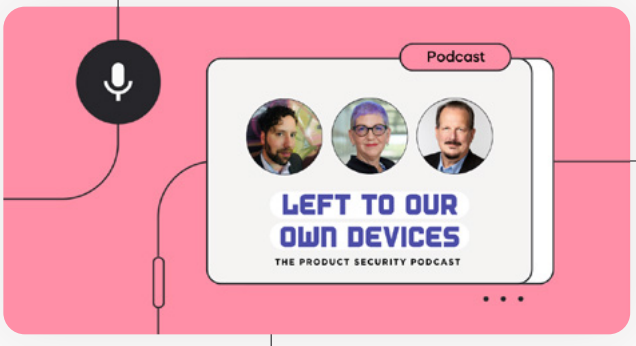
Blogs

Reflecting on Auto-ISAC: Main takeaways

Rolling Regulations: Embrace Them, Don't Chase Them

Keeping the Software Supply Chain Accountable with SBOMs

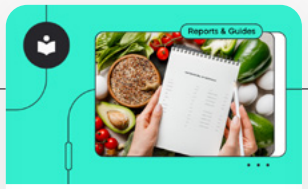
Podcasts



Knowledge Base

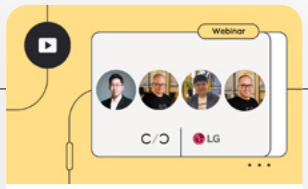
How to Automate Your CSMS for WP.29

Learn More →



SBOM for Connected Devices: Getting it Right

Learn More →



How LG Vehicle Component Solutions Keeps Automotive Products Secure

Learn More →

More about the Product Security Platform