August 2022

CYBELLUM

State of Automotive Cybersecurity 2022

A deep-dive into automotive cybersecurity risks and trends

Contents

01 / Introduction: Is the Automotive Industry Ready for the Next Phase of WP.29?

It hasn't been an easy year for cybersecurity pros in the automotive industry.

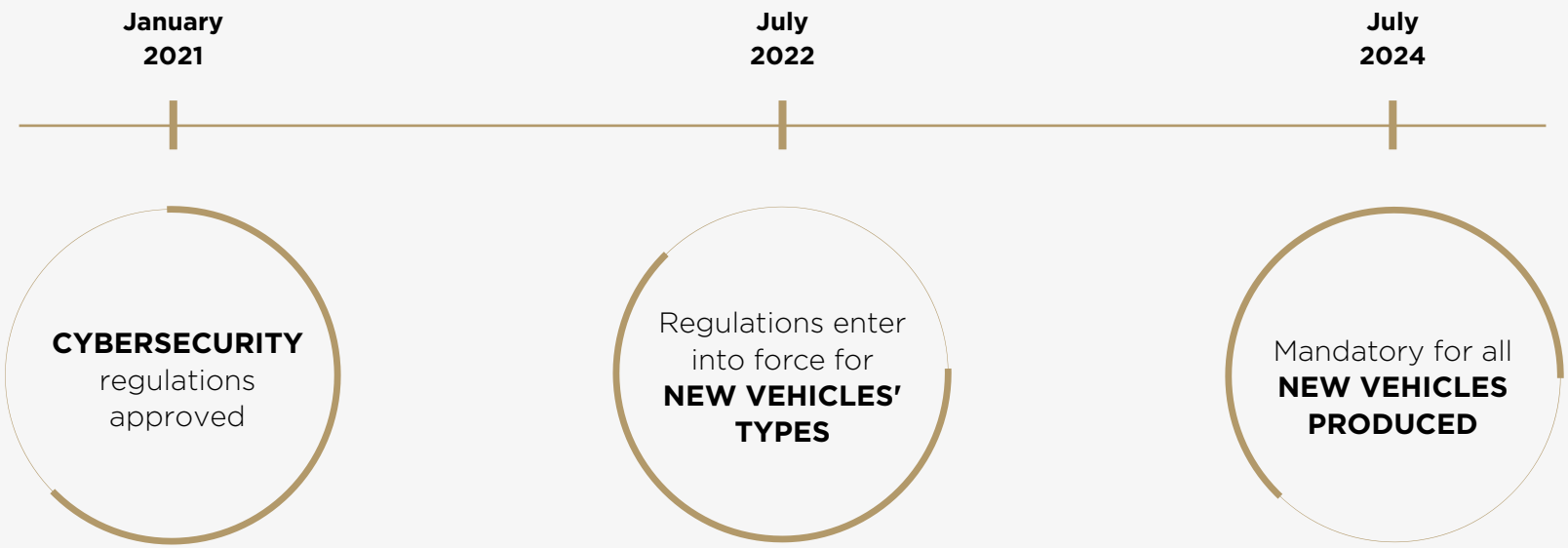
Hackers are increasingly setting their sights on connected automotive products – David Colombo's much-publicized ethical Tesla hack, a ransomware attack against Honda, and a suspected attack on a local Toyota supplier are only a few examples from the rapidly evolving threat landscape.

Then we have the rising risk to supply chain security due to reliance on complex software supply chains for connected vehicles, and recent supply chain shortages and breakdowns that push the automotive industry to rely on new and often un-vetted suppliers. The regulatory requirement for SBOMs is one of the ways to address supply chain security, but many teams are still struggling to find a way to generate a compliant SBOM that provide a complete system view, covering proprietary, third party, and open source code without slowing down production.

The next phase of WP.29 which came into direct effect this July, adds even more compliance and regulation requirements to product security teams already-heavy workload. As WP.29 demands automotive product security teams put a comprehensive CSMS (Cybersecurity Management System) in place, we wanted to provide the automotive product security community with insights and information on the current state of automotive cybersecurity, a look at the challenges to becoming WP.29 compliant, and provide insights and best practices for achieving cybersecurity.

> "WP. 29 is valid and mandatory for type approvals from July 2022 and the approvals are valid for three years. This is a tricky thing because it's a moving target, we don't know what will happen after those three years, but it is essential because we need to keep vehicles safe."
>
> Thomas Wambera, Affiliate Business Manager at AVL Deutschland

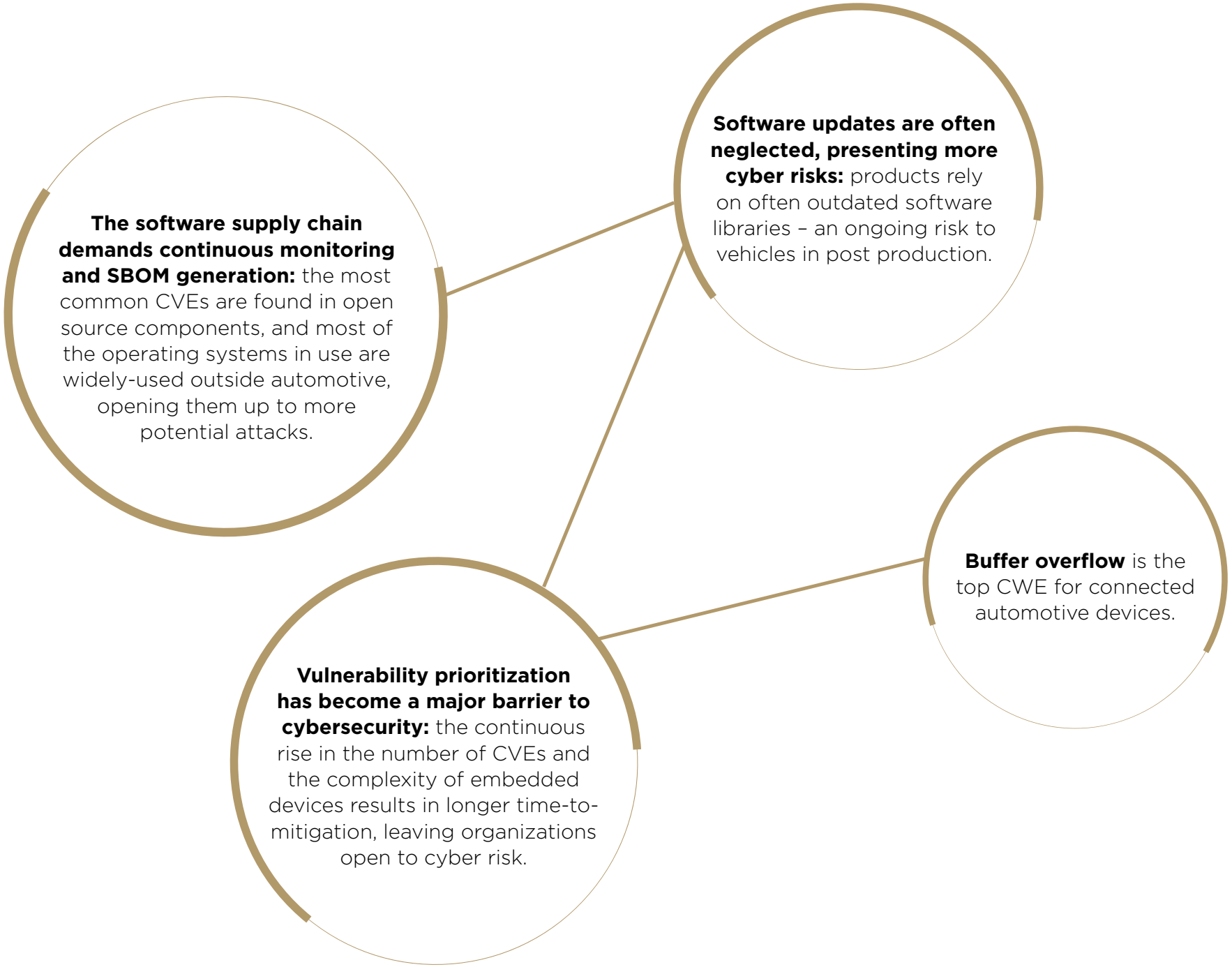
The timeline for WP.29



UN Reg. 155/156
Includes principle for CoC
for CSMS and SUMS

PCAutomotive Gap
Analysis Report

KEY TAKEAWAYS



02/

Supply Chain Security: The Long Road to Complete Visibility

A little over a year ago, the White House addressed the alarming rise in attacks on supply chains and issued the Executive Order on Improving Cybersecurity, accelerating the need for software developers and suppliers to generate up-to-date SBOMs containing all of their software components.

SBOMs help teams monitor their software for outdated and vulnerable components, and mitigate risks as soon as they are found. Looking at the data, it's clear that continuously generated SBOMs throughout the product lifecycle are critical for ensuring updated and vulnerability-free products.

03 / Open Source Software is Taking Over Connected Cars

As software continues to take over the automotive industry, managing software supply chain security is more important than ever.

Our research shows that the top 10 most popular components in use in automotive products in the past year were open source.

1. zlib
2. openssl
3. boost
4. sqlite
5. libpng
6. gcc
7. expat
8. libxml2
9. glibc
10. qt

Most common components being used in automotive products

> "Software nowadays is pretty much made up of components. 90% of the code that's in software, the code, was not written by the company you bought it from. It was written by third parties, sometimes commercial, oftentimes open source.
>
> So, you can say that the software developer nowadays doesn't really write software, they put some glue to put the components together, and that's their product."
>
> Tom Alrich, supply chain cybersecurity consultant

04/

Open Source Components: the Good, the Bad, and the Versions

While open source components help developers speed up processes by using software libraries created and maintained by a trusted community of developers, they also come with their own set of security risks.

When it comes to open source, traditional security testing tools aren't applicable. It's up to developers to track the security updates and advisories published across the open source community, and then make sure they quickly mitigate any vulnerabilities found in the open source software that they are using.

Our research shows that the most common CVEs detected in automotive components were in extremely popular open source components. It's also worth noting that most of the vulnerabilities are not new. The list consists of vulnerabilities from 2017, 2019, and 2020.

Looking at the data, it's clear that the chances are high your developers are using at least a few vulnerable software versions.

Vuln_id	Severity	Package
CVE-2020-12351	Medium	Sqlite
CVE-2016-2183	Medium	OpenSSL
CVE-2017-1000251	High	Sqlite
CVE-2016-0800	**Critical**	Sqlite
CVE-2017-1000250	Medium	Sqlite
CVE-2016-5195	High	Sqlite
CVE-2015-0235	**Critical**	Sqlite
CVE-2021-44228	Medium	libxml2
CVE-2016-6321	High	gcc
CVE-2016-2118	**Critical**	libpng

Most common CVEs detected in automotive products

05/

Notorious Open Source Vulnerabilities are Making Headlines – But Remain in Automotive Products

The notorious Log4j vulnerability and subsequent exploits that caught many top global enterprises by surprise in late 2021 proved once and for all that open source components can't be integrated and forgotten.

Unfortunately, although it made headlines, it appears that some ignored the call to update the vulnerable Log4j version: while not at the top of the list, Log4j joined the top 10 most common notorious vulnerabilities.

log4j and #1 on the list – BleedingTooth, are relatively recent, but it's concerning that the rest of the CVEs in this list date from 2014-2017.

Name	CVE
BleedingTooth	CVE-2020-12351
Sweet32	CVE-2016-2183
BlueBorne	CVE-2017-1000251
Drown	CVE-2016-0800
BlueBorne	CVE-2017-1000250
DirtyCow	CVE-2016-5195
Ghost	CVE-2015-0235
Log4Shell	CVE-2021-44228
Pointy Feather	CVE-2016-6321
Badlock	CVE-2016-2118

Most common "notorious/famous" CVEs detected in automotive products

06/ Keep Calm and Update: How Old Are Our Software Versions?

Since cyber attacks on connected devices are no longer a rare occurrence, and a public CVE provides hackers with a recipe and roadmap for exploits, we decided to look further than the vulnerabilities that caught headlines, and checked the amount of outdated software versions in use.

We found that **24%** of connected automotive products contain software versions that **are older than 10 years.**

Looking at the most common libraries in use that are over ten years old, we once again found that open source software is often neglected by product security teams.

Outdated and vulnerable versions in automotive products present one of the biggest challenges to the automotive industry, since they might affect vehicles that are already on the road.

As both regulation and threats evolve, it's critical that product security teams put tools and processes in place to ensure that this type of risk is mitigated as soon as possible.

1 zlib 2 expat 3 libpng 4 openssl 5 bzip2

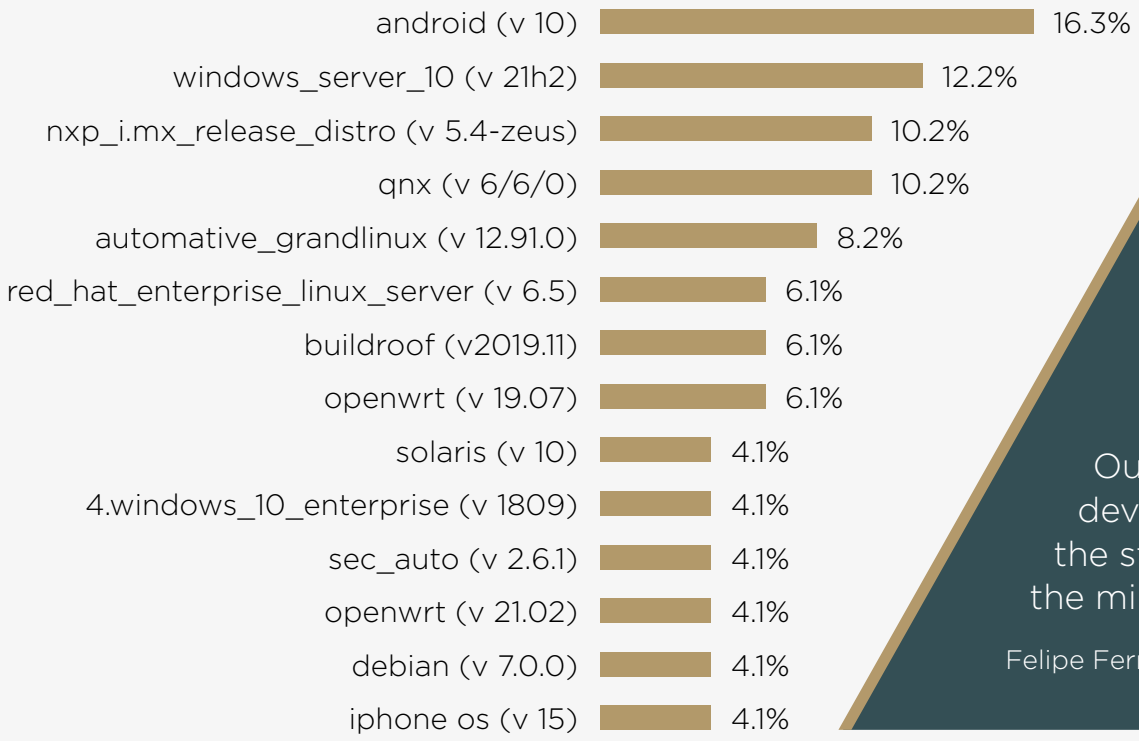
6 libxml2 7 xalan 8 iptables 9 ncurses 10 gcc

Most common libraries in use that are over ten years old

07 / The Operating Systems that Drive Connected Cars

Another interesting point uncovered in our research is that many automotive products use outsourced operating systems, including open source projects.

This adds another level of risk to connected automotive products, as relying on a widely-used OS provides potential attackers with a more easily accessible attack surface.



Most used operating systems, by % of software components using them

> "If you think about a tech company like Google – Android can carry thousands of vulnerabilities. Sometimes it can have big problems if it exposes user data, but you are not going to kill someone because of one vulnerability.
>
> Our environment is a little different. We are developing products that are going to be on the streets, at a speed that is not so low – so the mindset is different".
>
> Felipe Fernandes, Cyber Security Manager at Jaguar Land Rover

08/

So Many Vulnerabilities, So Little Time: Vulnerability Prioritization and Mitigation

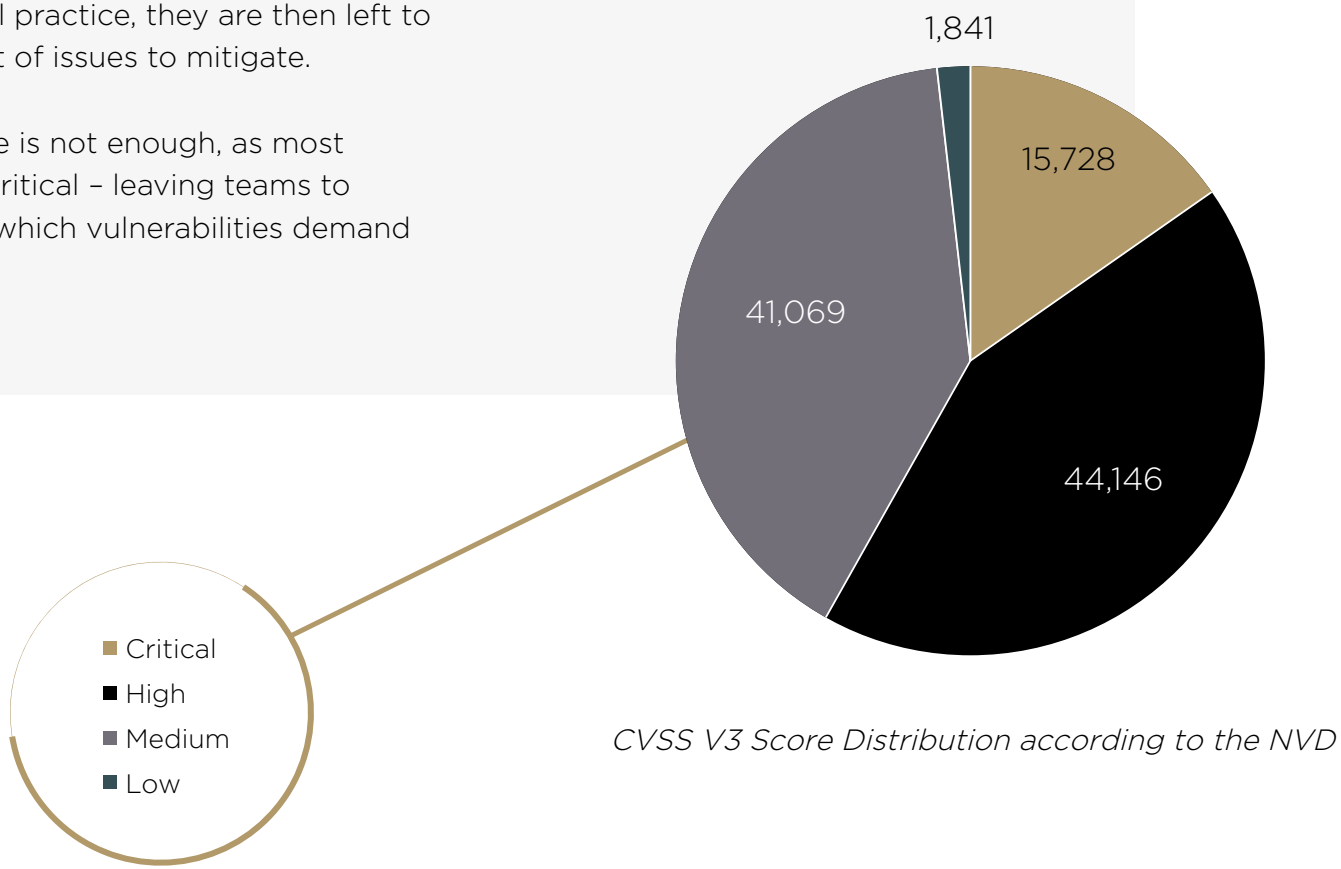
Detection is an important first step towards securing software – but then security and development teams must focus on the most critical issues, and mitigate them as quickly as possible.

We looked at the different types of published vulnerabilities to see how teams can speed up and scale their vulnerability management processes.

Prioritizing the Vulnerabilities that Matter Most

As the automotive software ecosystems become more and more complex, early and continuous monitoring for vulnerabilities is just the first step. Even if product security teams have tools and processes in place for this crucial practice, they are then left to deal with an increasingly long list of issues to mitigate.

Simply looking at the CVSS score is not enough, as most vulnerabilities are rated high or critical – leaving teams to sort through the list and decide which vulnerabilities demand immediate attention.



CVSS V3 Score Distribution according to the NVD

Source: https://nvd.nist.gov/general/nvd-dashboard

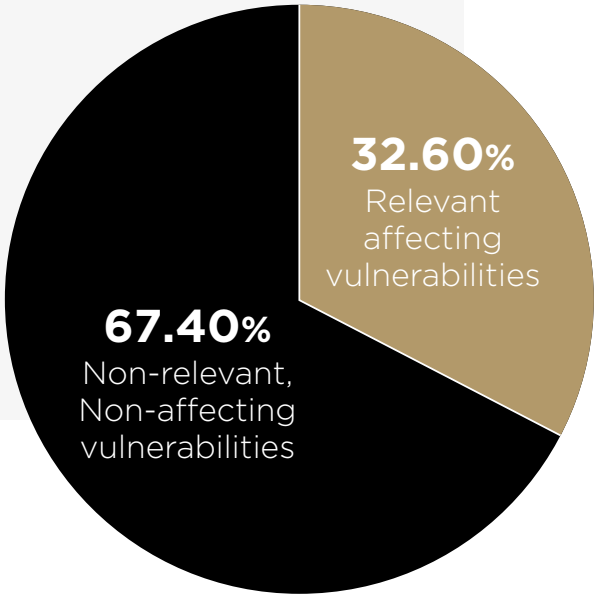
Prioritizing the Vulnerabilities that Matter Most

According to recent data, manual vulnerability management can take months, some research puts mitigation of high-severity vulnerabilities at nearly 250 days – an unacceptable timeframe, especially considering the ever-growing list of vulnerabilities.

In order to speed up and scale the vulnerability management process, it's crucial to focus on the vulnerabilities that matter most to your organization.

The good news is that we found that **only a third of detected vulnerabilities affect the product.**

Using advanced technology to analyze the vulnerabilities and cut down the long list is a crucial step in achieving quick mitigation.



Relevant vs. irrelevant CVEs based on contextual prioritization using Cybellum's Product Security Platform

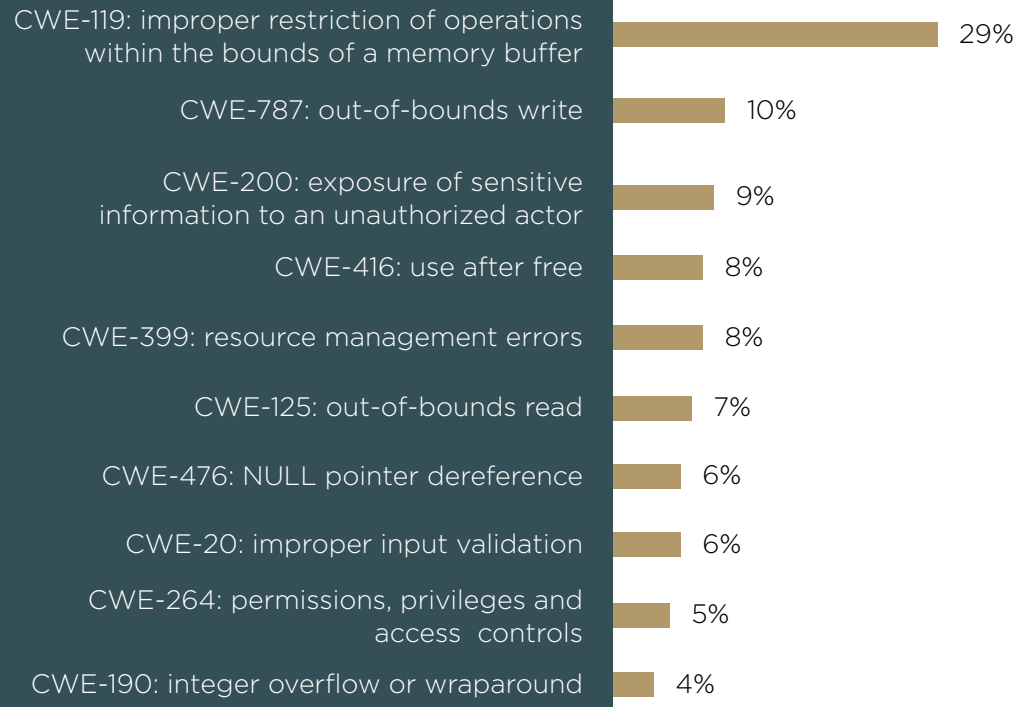
09/

Prioritizing Vulnerabilities: Looking Out for Top CWEs

Looking to the CVSS rating of a vulnerability used to be thought a good enough method for prioritization. However, the increasingly-complex connected device architecture and the ever-rising number of vulnerabilities, require new methods of prioritization.

Looking at the vulnerability type (CWE), can provide product security and incident response teams with valuable information on how exploitable a vulnerability is, and what its impact can be.

According to our findings, these were the top seven CWEs in automotive products over the past year.



10 / WP.29: What's Next for Automotive Cybersecurity?

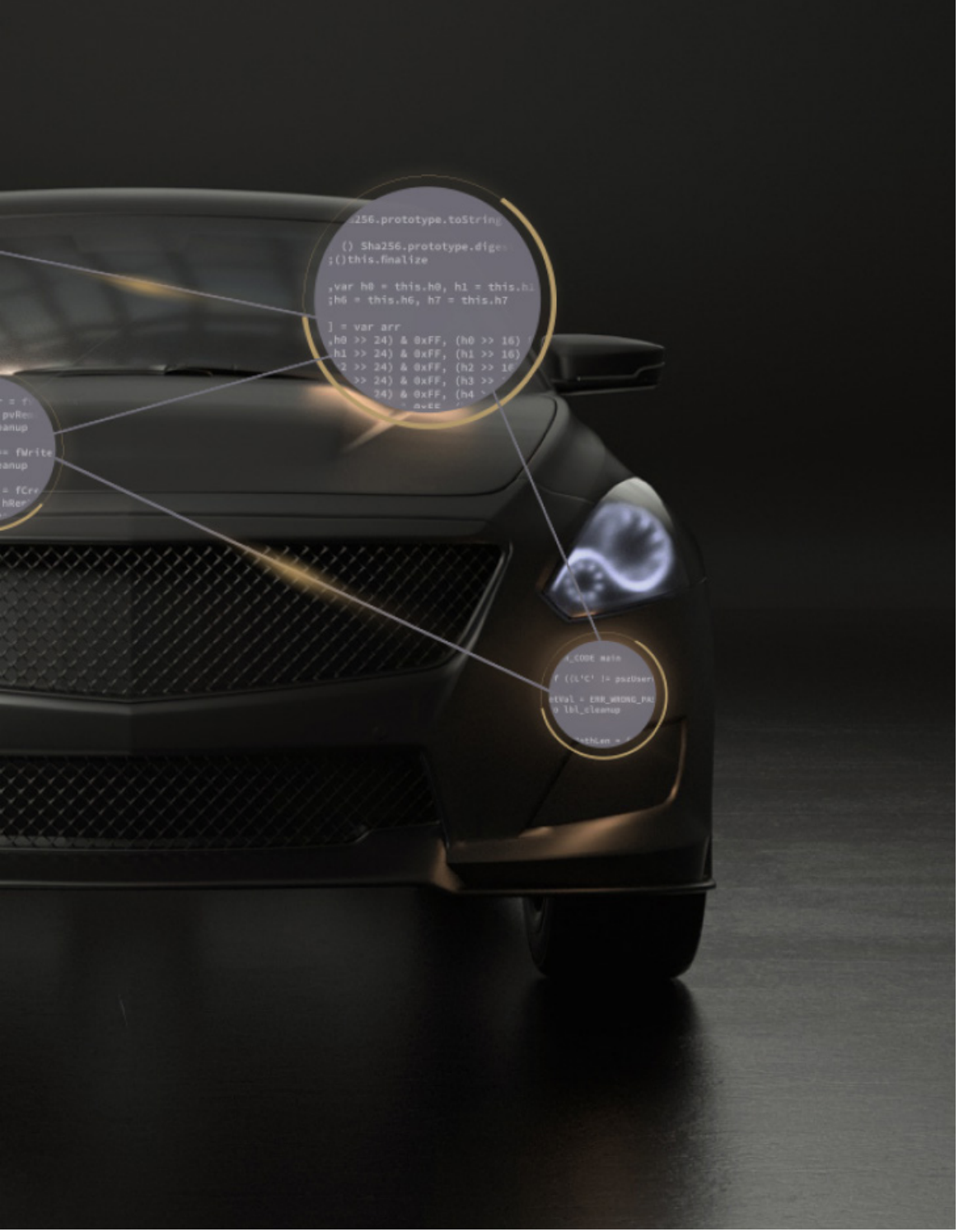
If a rapidly evolving cyber threat landscape wasn't enough of a challenge, increased cybersecurity regulation adds even more tasks to product security teams' already heavy workload.

Currently a top concern for automotive teams is one of the most important regulation updates to come out over the past few years – WP.29, which came into force in January 2021 and is binding in the EU from July 2022, followed by the next phase of WP.29 which will come into effect in 2024.

WP.29 puts the responsibility for cybersecurity certification on the manufacturers. It demands the incorporation of best practices in the design of vehicles and hold manufacturers responsible for the cybersecurity of their vehicles. It also requires ongoing cybersecurity for vehicles throughout all stages of the vehicle's lifecycle, including years of driving on the road.

That means that the practice of generating an SBOM is no longer enough. While it's a crucial first step in supply chain and product security, it is far from the only one. WP.29 addresses many of the risks mentioned in our findings, like monitoring outdated software, putting incident response processes in place, and more.

In order to ensure product security from design and development, to delivery and post production, a comprehensive cybersecurity strategy is critical.



11/

Fusing Cybersecurity Into all Stages of the Product Lifecycle

As product security teams in the automotive space continue to work hard to achieve cybersecurity and compliance, continuously faced with new challenges, it's critical to put a mature cybersecurity strategy in place.

This requires implementing new processes and policies from the earliest stages of development all the way to post-production.

Cybellum's Product Security Platform helps product security pros speed up and scale cybersecurity throughout the entire product lifecycle – from SBOM's, to vulnerability management and incident response.

To book a meeting **with one of our cybersecurity and cyber-compliance experts, visit** cybellum.com/schedule-a-demo