

More Than Half the Code Running Cars Carries a Known Vulnerability, and the EU Countdown Starts in 2 Days

More than half of the open-source software stack behind software-defined vehicles carries a known security flaw.

BERLIN, GERMANY, September 9, 2026 /EINPresswire.com/ -- More than half of the open-source software stack behind modern software-defined vehicles carries a known vulnerability. And due to EU CRA rules — the companies shipping it, now face a 24-hour reporting deadline backed by fines of up to 15 million EUR.

[A new benchmark from DerScanner](#) scanned 43 open-source components from the Eclipse SDV, KUKSA, COVESA and Velocitas projects, resolving 8,821 dependencies in total.

The results are terrifying:

- 55% of resolved dependencies carry a known vulnerability,
- adding up to 660 distinct CVEs, 333 of them critical.
- And at least 1 critical finding appeared in 30 of the 43 components.

In two days, on 11 September 2026, [EU Cyber Resilience Act](#) obligations take effect for manufacturers placing products on the EU market. Actively exploited vulnerabilities must be reported within 24 hours. And the penalties reach 15 million euro or 2,5% of worldwide annual turnover, whichever is higher.

A separate layer of risk across the same codebases involves packages that generate no CVE at all. The benchmark found 826 packages:

- 671 of which were abandoned with zero maintenance activity,
- 311 impersonating a more popular project through starjacking,
- 124 typosquatting a well-known package name,
- 30 surviving on a single maintainer,
- and 18 with a version documented to have shipped malicious code. It includes debug, mongodb and jsdom, utilities found in projects everywhere.

Automotive feels the pressure first, since the Cyber Resilience Act turns supply chain hygiene into a compliance problem with a price tag. The underlying pattern runs much wider. Black Duck reported that 65% of organizations surveyed in 2025 had experienced a software supply chain

attack in the prior year, and the OWASP Top 10 (2025) added Software Supply Chain Failures as a Top 3 category, ranked first by half of community survey respondents.

Every critical finding in this corpus entered through a dependency the engineering team never selected. A manifest review shows the libraries developers deliberately added. The dangerous code sits deeper in the tree, in packages nobody chose.

Fabian Dechant
Automotive Industries
[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/940827626>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.