

# Automotive Vulnerability Analysis System (VERZEUSE for SIRT)

Panasonic

## Benefits

### Reducing Vulnerability Response Costs

Currently, 30,000 vulnerabilities are reported annually, leading to increasing response costs. To address these vulnerabilities,

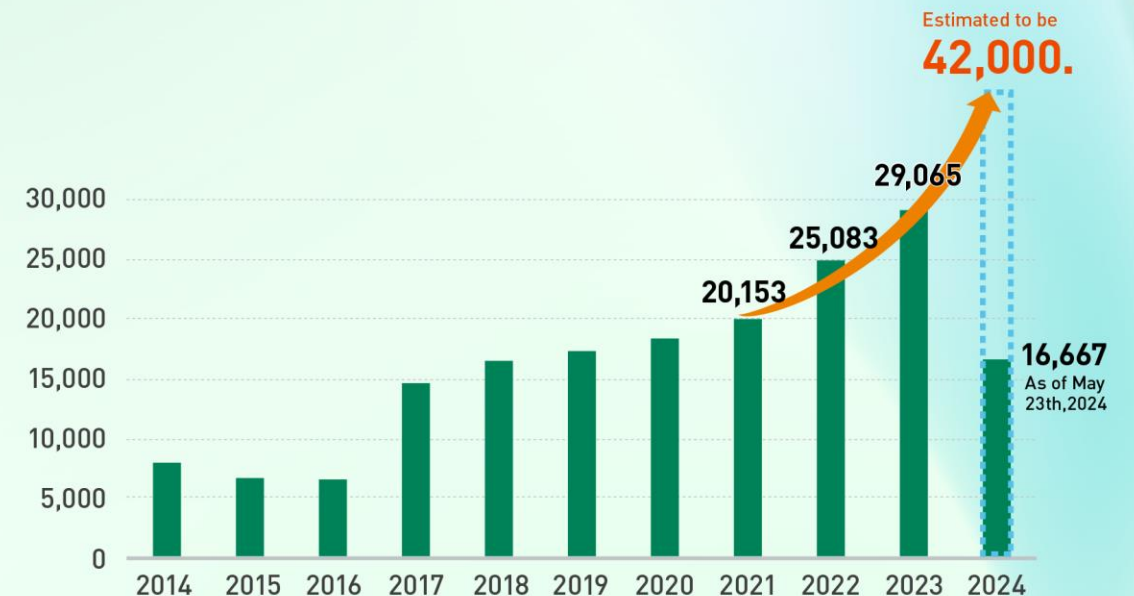
1. We analyze the risks to actual vehicles based on vulnerabilities.
2. We prioritize the vulnerabilities that require immediate attention.

This approach enhances the efficiency of vulnerability response process.

### Ensuring Vehicle Safety and Security Against Cyber Attacks

We mitigate drivers' concerns about cyber attacks exploiting vulnerabilities, ensuring that drivers can operate their vehicles safely and securely.

The number of vulnerabilities is increasing year by year.



Source : CVE Details (<https://www.cvedetails.com/browse-by-date.php>)



VERZEUSE is our brand of cybersecurity technologies and services that combat cyber-attacks.

# Automotive Vulnerability Analysis System (VERZEUSE for SIRT)

Panasonic

## Technical Advantages

### Automated Risk Analysis for Vehicle Vulnerabilities

We analyze risks of vulnerabilities at the ECU level and evaluate their impact on the entire vehicle, considering vehicle configuration and ECU interdependencies. This enables appropriate prioritization of vulnerabilities based on their actual risk levels. Additionally, our analysis steps comply with ISO 21434 standards.

### Cross-Industry Cyber Threat Intelligence Collection and Utilization

The Panasonic Group has extensively accumulated Cyber Threat Intelligence (CTI) through its security services for Factories, Buildings, and Smart Houses. Leveraging this knowledge, we provide analysis logic based on the latest threat scenarios.



# Automotive Vulnerability Analysis System (VERZEUSE for SIRT)

Panasonic

## Applications

### Cloud-Based Vulnerability Analysis System

Users can perform analyses using intuitive GUIs, manage the status of analyses collectively, and generate comprehensive analysis reports.

### Vulnerability Analysis Support Service

Our security experts provide support for vulnerability analysis. We also assist with Threat Analysis during vehicle design, ensuring consistent vulnerability analysis based on the threat analysis results.



The screenshot displays the VERZEUSE web application interface. At the top, there is a navigation bar with tabs for Dashboard, Incident, Vulnerability, Survey, Analysts, KPI, CTI, and Task. The main content area is divided into several sections:

- Vulnerability No. CVE-2024-6387**: Shows details for a specific vulnerability, including Created Time (2024/07/02 18:00), Base Score (8.1 HIGH), Published Date (2024/07/01), and Status (In Progress). It also indicates the progress (50%), Priority (High), and Impact (Severe).
- Vehicle List**: A table listing various vehicle models and their associated risk levels. For example, VEHICLE-1 through VEHICLE-5 are listed with a risk level of 4: High, while IVI and Multimedia are listed with a risk level of 4: High.
- VEHICLE-5**: A detailed view of a specific vehicle model, showing its status (In Progress), progress (50%), priority (High), and due date (2024/09/30). It includes a scenario (VAS-106) and a table of vehicle details: Model (Z), Grade (2023-03), Region (Asia), Platform (PF-004), Shipped (300,000), and SBOM Updated At (2024/07/01).
- External interface Layer**: A diagram showing the architecture of the vehicle's external interface layer, including components like On-board Charger, OBD, TMS, and various interfaces (Can-1, Can-2, etc.).
- VEHICLE-5 > Multimedia**: A detailed view of the multimedia system, showing its status (Analyzed), progress (80%), priority (High), and due date (2024/08/31). It includes a scenario (EAS-108) and a table of ECU details: ECU Name (Multimedia), Model Code (IVIM-001), and Supplier (VEND-W).
- Attack Scenario**: A table listing attack scenarios, such as EAS-108, which describes a remote control app leaking FlashMemory user information, affecting privacy.



VERZEUSE is our brand of cybersecurity technologies and services that combat cyber-attacks.