"Pwn2Own Automotive 2024" - VicOne & ZDI lead first hackathon to uncover cyber vulnerabilities in connected vehicles to a great success

VicOne and sponsors including Tesla announced the discovery of 49 unique bugs in-vehicle infotainment systems, EV chargers, modems, etc. and awarded US$1,323,750 to security researchers

Tokyo/Munich, January 31, 2024 - VicOne, a leading provider of automotive cybersecurity solutions, hosted "Pwn2Own Automotive 2024", its first ethical hacking event exclusively for the automotive sector, at Automotive World in Tokyo (January 24-26, 2024) to explore and address cybersecurity challenges in the automotive industry. The event was dedicated to discovering and fixing digital security vulnerabilities of connected cars and, thus, the cybersecurity of vehicles. It was a great success. Specifically, 17 white hat hacker teams/individuals from 9 countries, including Germany, participated in a total of over 50 entries both remotely and on-site in 4 categories: "Tesla," "In-Vehicle Infotainment (IVI)," "EV Chargers," and "Operating System," and the participants competed for cash and prizes worth US$1,323,750. A total of 49 unknown security vulnerabilities (zero-day vulnerabilities) were discovered by the participants over the three days. To win, participants had to take advantage of newly discovered vulnerabilities to attack target systems and devices and execute arbitrary instructions. However, the event was not only about prestige and competition between the best white hat hackers on the scene, but also about collaboration within the automotive industry and with external IT cybersecurity experts to make the entire industry safer.

VicOne's parent company, global cybersecurity leader Trend Micro™, co-hosted the event through the Zero Day initiative™ (ZDI), the world's largest vendor-agnostic bug bounty program. Electric vehicle manufacturer Tesla, as the main sponsor of the event, put its own products to the test including a modem, infotainment system, and Model Y vehicle. Individual hackers and hacking teams from countries such as Vietnam, the USA, and Japan, but also from the UK, Hungary, the Netherlands, France, and Germany took part. From Germany, for example, Team Tortuga (remotely) and fuzzware.io (onsite) took part and carried out their hacks.

The hackers from fuzzware.io targeted the Sony XAV-AX5500 and the Alpine Halo9 iLX-F509 in the In-Vehicle Infotainment (IVI) category, as well as the ChargePoint Home Flex, the Autel MaxiCharger AC Wallbox Commercial, the EMPORIA EV Charger Level 2 and the Phoenix Contact CHARX SEC-3100 in the Chargers for Electric Vehicles category. With no less than six hacking attempts, they were among the most diligent hackathon participants. Team Tortuga checked the ChargePoint Home Flex in the category chargers for electric vehicles for possible security vulnerabilities. With a total profit of *US$*177,500, the German fuzzware.io team took a very good second place and was only beaten by the winning team Synacktiv from France with a total profit of *US$*450,000, who now holds the title of "Master of Pwn."

The multinational event also served to connect and engage the automotive industry with the cybersecurity industry. Hacking events like this are crucial to prepare the global automotive industry for the evolving threat landscape. For example, the ongoing on-site competition also featured attack scenarios that emphasized the importance of discovering cybersecurity vulnerabilities and the potential threats that can arise if vulnerabilities are not addressed promptly. Early detection of vulnerabilities and sharing them with vendors for their countermeasures is important, first and foremost, from the standpoint of safety and cost. By uncovering vulnerabilities in their own products, participating companies were able to gain insights into how they can develop more secure and reliable products. The zero-day vulnerabilities discovered through this competition will be reported to the respective vendors for further action to fix them. Details of the vulnerabilities will be announced 120 days or later after the conclusion of the competition based on their status. The event revealed the very latest security research and hacking approaches and, therefore, has at least indirect relevance for planned government and industry security measures and regulations in the EU.

"With the constant innovations in the automotive industry, the car is not only a traditional means of transportation but also a completely new mobility and a new living space. In an era where our lives and mobility are becoming more closely connected through the Internet, cybersecurity is of paramount importance for people's economic and physical safety, which is why it is essential to identify and address security vulnerabilities in systems before malicious attackers do. Pwn2Own Automotive 2024 is one of VicOne's efforts to spread its long-standing security expertise to the automotive industry.", said Max Cheng, CEO of VicOne. "We are also delighted that the number of entries far exceeded our expectations. This was a very successful demonstration that we are at the forefront of discovering zero-day vulnerabilities in the automotive industry and protecting against cyber-attacks, thanks to the dedication and expertise of our participants and the great work of our own researchers. We would like to thank everyone who attended this event and shared the spirit of security research and innovation. This is not a one-time event. VicOne will continue to host this event, and I hope I can see everyone again at 2025 Pwn2Own Automotive Tokyo."

"Since 2007, Pwn2Own has been the world's largest hacking contest, rewarding the world's top researchers with the ability to penetrate the world's most challenging attack surface and discover zero-day vulnerabilities. While previous competitions have covered a wide range of areas, this year's competition was the first Pwn2Own to focus on automobiles. The discovery of 49 new unknown vulnerabilities and the opportunity to bring together a community of automotive vendors and world-class security researchers to share the latest and most valuable insights into automotive cybersecurity is of critical importance to the global

researchers to share the latest and most valuable insights into automotive cybersecurity is of critical importance to the global automotive industry's ability to prepare for evolving threats." explains Brian Gorenc, VP of Threat Research at VicOne's parent company Trend Micro and responsible for the ZDI program.

For more updates on the Pwn2Own Automotive and future Pwn2Own hacking events, follow the social media accounts and blog posts from VicOne (LinkedIn, X, blog) and ZDI (LinkedIn, X, blog).

About VicOne:
With a vision to secure the vehicles of tomorrow, VicOne offers a broad portfolio of cybersecurity software and services for the automotive industry. VicOne's solutions are specifically designed to meet the stringent requirements of automotive manufacturers and are engineered to meet the unique needs of modern vehicles. As a subsidiary of Trend Micro, VicOne is built on a solid foundation in cybersecurity resulting from Trend Micro's 30+ years of experience in the industry. VicOne provides unparalleled protection for the automotive industry and deep security expertise that enables our customers to build safe and smart vehicles. For more information, please visit vicone.com.

---

https://newsroom.trendmicro.com/2024-01-31-Pwn2Own-Automotive-2024-VicOne-ZDI-lead-first-hackathon-to-uncover-cyber-vulnerabilities-in-connected-vehicles-to-a-great-success