Anybody Can Hack Tesla Model 3 And Steal It Or Crash It Remotely As Tesla Chinese Curse Grows Worse

By

Sergiu Gatlan

- 0

Fluoroacetate is the team which won the competition earning $375,000 out of the total of $545,000 earned by security researchers who demoed their research during this year's Pwn2Own Vancouver 2019.

During the last day, Fluoroacetate's Amat Cama and Richard Zhu successfully targeted and successfully hacked their way into a Tesla Model 3's Chromium-based infotainment system as part of their automotive category demo, using "a JIT bug in the renderer to display their message."

This brought them $35,000 out of their total of $375,000 in cash collected during the three days of Pwn2Own and, of course, the Tesla Model 3 they successfully hacked into during their research demo.

The same duo of researchers also managed to demo exploits for Apple Safari, Oracle VirtualBox, VMware Workstation, Mozilla Firefox, and Microsoft Edge, allowing the Fluoroacetate team to dominate the competition, overshadowing the earnings of all other contestants.

Team Fluoroacetate

This is not the first time Fluoroacetate won the Pwn2Own competition seeing that they also were the ones with the most points collected after the end of last year's Pwn2Own which took place in Tokyo during November, and brought them $215,000 and the title of "Master of Pwn."

Day three was also supposed to be the day when Team KunnaPwn playing field, with an attempt at hacking the "VCSEC component of the Tesla Model 3 in the automotive category" but they withdrew from the competition.

The full schedule for the day and the results following each exploitation attempt are listed in the table below.

Challenge	Result
1000 - Team KunnaPwn targeting the VCSEC component of the Tesla Model 3 in the automotive category.	**Withdrawn:** - The Team KunnaPwn team has withdrawn their entry from the automotive category.
1300 - Fluoroacetate (Amat Cama and Richard Zhu) targeting the infotainment system (Chromium) on the Tesla Model 3 in the automotive category.	**Success:** - The Fluoroacetate duo used a JIT bug in the renderer to win $35,000 and a Model 3.

According to Trend Micro's Zero-Day Initiative, the organizers of the Pwn2Own contest, "As always, onsite vendors have received the details of these bugs and now have 90 days to produce security patches to address the issues we reported."

As part of the first day of Pwn2Own, contestants were able to hack into the Apple Safari web browser, Oracle's VirtualBox, and VMware Workstation, being rewarded with $240,000 in cash awards for their efforts.

During the second day of Pwn2Own, researchers successfully pwned Mozilla's Firefox and Microsoft's Edge web browsers, as well as VMware's Workstation client, earning them a total of $270,000 in cash awards.

An error occurred.

Try watching this video on www.youtube.com, or enable JavaScript if it is disabled in your browser.

Related Articles: