Summarizing the Pwn2Own 2019: Safari, VirtualBox was 'pierced' on the first day, Firefox, Edge on the second day and Tesla Model 3 'closed the window'

Pwn2Own is a computer hacking competition held annually during the CanSecWest security conference, starting in 2007, challenged candidates to exploit widely used mobile software and devices with holes Unknown vulnerabilities before.

Pwn2Own is a hack contest held annually in the framework of the CanSecWest security conference, which began in 2007. The challenged candidates exploited widely used software and mobile devices with vulnerabilities. known before. Pwn2Own this year is held in Vancouver, Canada. Summarizing the three-day event, Fluoroacetate was the overwhelming victory team with a reward of up to 375,000 dollars out of a total of 545,000 dollars that all security researchers pocketed at Pwn2Own Vancouver this year.

1. The 13-year-old 'Hacker' enters the school's computer system to create a 'list of the most hated kids'

Until the third day, ie the last day of the event, the teams will compete in the automotive category, and the two famous security researchers Amat Cama - Richard Zhu of Fluoroacetate team continue to create surprises. when targeting and successfully hacking the infotainment system based on Chromium kernel on Elon Musk billionaire Tesla Model 3 electric scooter, and the general 'scenario' is still using "JIT error in the renderer to display the

hack message '.

This work has brought to two researchers a bonus of up to 35,000 USD, contributing to the figure of 375,000 dollars that Fluoroacetate has pocketed after 3 days of Pwn2Own. And of course, the Tesla Model 3 model they successfully hacked is part of the demo in this team's own research work.

Besides Tesla Model 3, Fluoroacetate researchers have also successfully exploited demo holes for Apple Safari, Oracle VirtualBox, VMware Workstation, Mozilla Firefox and Microsoft Edge . Strengthening the dominance of this security group in Pwn2Own periods in general and Pwn2Own 2019 in particular, and overshadowing many research works are also very noticeable of other candidates.

1. If using an Android phone, be careful: You may be being tracked without knowing

As said, this is not the first time Fluoroacetate won at a Pwn2Own period. In last year's event in Tokyo in November, the security team was also the one who won the most points after three days of competition, pocketing a total of $ 215,000 and also holding the title " Master of Pwn.

Returning to Pwn2Own 2019, the third day of competition is also expected by many to be Team KunnaPwn's own 'stage', in an effort to hack "the VCSEC system of the Tesla Model 3 in the automotive category", but eventually they withdrew from the competition and the results were, as we know, the stage once again belonged to Fluoroacetate.

The full schedule for the third day of the Pwn2Own 2019 and the final results are listed in the table below:

Exam Team Results 1000 - Team KunnaPwn targets the Tesla Model 3 VCSEC entertainment system in the automotive category. KunnaPwn withdrew from the automotive category at the end of 1300 - Fluoroacetate (Amat Cama and Richard Zhu) targeted the infotainment system (Chromium) on Tesla Model 3 in the automotive category. Success: - The duo of Fluoroacetate used the JIT error in the renderer to win $ 35,000 and a Model 3.

According to organizers of the Pwn2Own contest, "as always, after giving bonuses to security researchers, companies with products that have been successfully hacked will receive detailed information about security vulnerabilities and there are 90 days to deploy security patches to address reported issues ".

1. Mozilla Firefox and Microsoft Edge browsers were lost at the Pwn2Own 2019 hack contest

In the first day of the Pwn2Own 2019, the contestants successfully hacked into Apple Safari web browser, Oracle's VirtualBox and VMware Workstation, receiving a total of $ 240,000 in bonuses from the product providers.

In the second day of the event, Fluoroacetate has targeted and successfully exploited security vulnerabilities on Mozilla's Firefox web browser and Microsoft's Edge. With these two successful exploits of security vulnerabilities, Fluoroacetate has collected a total of $ 180,000 ($ 40,000 from Mozilla and $ 130,000 from Microsoft) in the second day of Pwn2Own 2019, combined with $ 160,000 from the previous day, they had $ 340,000 after 2 days of the event. Besides, in addition to the $ 35,000 bonus for successful hacking of Tesla Model 3, the Fluoroacetate team will also be rewarded with a completely new Model 3 (after Tesla successfully patched the hole). this car). Besides, another "forgotten" name from Exodus Intelligence team: Arthur Gerkis also successfully exploited the Microsoft Edge vulnerability related to logical errors, helping to escape Edge's sandbox environment. This work earned Arthur Gerkis a prize of up to 50 thousand USD. Another well-known security expert, Niklas Baumstark, also targeted Mozilla's Firefox web browser and successfully exploited the logic-related JIT vulnerability to get rid of the browser sandbox environment and pocketed $ 40,000. la bonus.

In sum, in the first two days of the Pwn2Own Vancouver 2019 event, participants received a total of $ 510,000 cash prizes for 8 successful exploits and hacks of popular software. like Safari, Firefox, Microsoft Edge, VMware Workstation and Virtualbox. And the situation of the third day is as we know it.

1. There were 12,449 serious data breaches recorded in 2018, an increase of 424% compared to 2017

This year's event marks the first time that the Pwn2Own automobile category with the award has appeared "ranging from 35,000 to 300,000 dollars depending on many factors related to the complexity and severity of The vulnerability has been exploited, as are the hacking techniques used. "