Tesla Hacked Twice at Pwn2Own Exploit Contest

Researchers at French offensive hacking shop Synacktiv have demonstrated a pair of successful exploit chains against Tesla's newest electric car to take top billing at the annual Pwn2Own software exploitation contest.

Pwn2Own organizers confirmed the successful hacks exploited flaws in the Tesla-Gateway and Tesla-Infotainment sub-systems to "fully compromise" a new Tesla Model 3 vehicle.

The first Tesla hack, described as a TOCTOU (time-of-check to time-of-use) race condition, earned the hackers a $100,000 cash prize and ownership of the compromised car. Synacktiv said the Tesla Model 3 gateway was fully compromised from the ethernet network.

SecurityWeek sources say Tesla security response team was on site at the event and validated the findings. The company is expected to issue fixes via the vehicle's self-updating system.

On the second day of the contest in Vancouver, Canada, Synacktiv's researchers created an exploit chain that used a heap overflow and an out-of-band (OOB) write vulnerability to pop the Tesla-Infotainment system. The hack was described as "Unconfined Root" and scored the Synacktiv team a $250,000 cash prize.

Image credit: Zero Day Initiative

Tesla is a Pwn2Own co-sponsor and is using the annual contest to incentivize security researchers to showcase complex exploit chains that can lead to complete vehicle compromise.

This isn’t the first time Tesla has sought to attract the attention of advanced exploit writers at Pwn2Own. Back in 2019, the company gave away a Tesla Model 3 to a pair of researchers demonstrating successful exploits and this year the organizers plan to raise the level of complexity of what constitutes a successful car-hacking exploit.

This year, the organizers were looking to attract exploits targeting Tesla’s Tuner, Wi-Fi, Bluetooth or Modem components.

Related: Tesla Returns as Pwn2Own Hacker Takeover Target

Related: Pwn2Own 2019: Researchers Win Tesla After Hacking Its Browser

Related: $200,000 Awarded for Zoom Zero-Click Zoom Exploit at Pwn2Own

Related: Over $1.1 Million Awarded at Pwn2Own 2022 for 25 Zero-Day Vulns

https://www.securityweek.com/tesla-hacked-twice-at-pwn2own-exploit-contest/