

محقق امنیتی با کشف آسیب‌پذیری مرورگر سافاری برنده جایزه ۱۰۰ هزار دلاری شد - دیجیاتو

ایمان صاحبی | یکشنبه، ۲۲ فروردین ۱۴۰۰

یک محقق امنیتی با شرکت در مسابقه هک Pwn2Own توانست یک آسیب‌پذیری جدی تک‌کلیکی را در مرورگر سافاری اپل پیدا کند و به عنوان جایزه، ۱۰۰ هزار دلار با خود به خانه ببرد.

به گزارش گروه [Zero Day Initiative](#)، مسابقه Pwn2Own امسال از تاریخ ۱۷ فروردین آغاز شد. در روز اول «جیک دینز»، محقق شرکت RET2 Systems آسیب‌پذیری مهمی را در مرورگر سافاری اپل پیدا کرد. همان طور که در تصویر زیر پیداست، دیتز با کمک سرریز عدد صحیح و نوشتن یک کد خارج از قاعده توانست به اجرای کد در سطح کرنل دست پیدا کند.

این محقق امنیتی در نهایت ۱۰۰ هزار دلار بابت کشف این آسیب‌پذیری دریافت کرد و در مسابقه ۱۰ امتیاز پیش افتاد. Zero Day Initiative هر سال از رقابت Pwn2Own میزبانی می‌کند. این گروه محققان امنیتی زیادی را از سراسر دنیا گردآوری می‌کند تا آن‌ها در سیستم عامل‌ها و پلتفرم‌های بزرگ به دنبال آسیب‌پذیری بگردند. از دیگر نرم‌افزارهای هدف در مسابقه امسال Pwn2Own می‌توانیم به زوم، گوگل کروم و مایکروسافت اج اشاره کنیم.

با وجود این که محصولات اپل معمولاً هدف محبوبی در مسابقات Pwn2Own نیستند، اما این نخستین باری نیست که در طول این رویداد مشکلی در سافاری کشف می‌شود. قبلاً در مسابقات سال‌های ۲۰۱۸ و ۲۰۱۹ هم آسیب‌پذیری‌هایی در مرورگر اپل کشف شده بودند.

رویداد Pwn2Own اولین بار در ماه آوریل سال ۲۰۰۷ در ونکوور کانادا برپا شد. گوگل در سال ۲۰۱۲ از حمایت از این رویداد خودداری کرد چون شرکت‌کنندگان در قوانین آن به تشریح روش‌های کشف آسیب‌پذیری‌ها ملزم نشده بودند. این شرکت در آن سال مراسم جداگانه‌ای با نام Pwnium را برای خودش برگزار کرد تا محققان امنیتی مشکلات مرورگر کروم را پیدا کنند. با این حال، در سال ۲۰۱۳ با همکاری Zero Day Initiative و گوگل قرار شد هکرها روش‌های نفوذ خود را تشریح کنند تا گوگل دوباره حاضر به حمایت از این مراسم شود.

[دیجیاتو](#)