Big browsers fall in Pwn2Own exploit competition

March 22 2015, by Nancy Owano

Name any of the big browsers and there's an exploit for it. All four major browsers fell down during the Pwn2Own hacking competition running concurrently with the CanSecWest 2015 Conference in Vancouver, British Columbia. That meant showdowns on Internet Explorer, Chrome, Safari and Firefox. All four were unable to survive exploits at the event. The Pwn2Own drew security researchers who attempted exploits in 30 minutes, as per requirements, in return for cash.

Contestants worked on fully patched browsers. The HP Security Research Zero Day Initiative researchers do this contest each year at the CanSecWest security conference. According to the rules, entries should be designed to leverage a vulnerability to modify the standard execution path of a program or process to allow the execution of arbitrary instructions. The entry is required to defeat the target's techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) and application sandboxing. The resulting payload should be executing in an elevated context (for example, on Windows-based targets, Medium integrity level or higher).

To compromise a target during the contest, a contestant has a 30-minute time slot to complete the attempt, not including time to set up possible network or device prerequisites. A successful remote attack must require no user interaction beyond the action required to browse to the malicious content and must occur within the user's session with no reboots, or logoff/logons.

If a sandbox is present, a full sandbox escape is required to win. A given vulnerability may only be used once across all categories. The initial vulnerability utilized in the attack must be in the registered target. The sandbox escape utilized in the attack must be in the registered target (unless the attack leverages a SYSTEM-level privilege escalation).

The final count for exploits was four in Internet Explorer 11, three in Mozilla Firefox, two in Apple Safari and one in Google Chrome. Reporting on the exploit that took down Chrome, Dustin Childs of HP Security Research said JungHoon Lee (lokihardt) showed an exploit for both stable and beta versions of Chrome.

"He leveraged a buffer overflow race condition in Chrome, then used an info leak and race condition in two Windows kernel drivers to get

SYSTEM access. With all of this, lokihardt managed to get the single biggest payout of the competition, not to mention the single biggest payout in Pwn2Own history: $75,000 USD for the Chrome bug, an extra $25,000 for the privilege escalation to SYSTEM, and another $10,000 from Google for hitting the beta version for a grand total of $110,000. To put it another way, lokihardt earned roughly $916 a second for his two-minute demonstration. There are times when "Wow" just isn't enough."

Outside HP, tech sites largely agreed that Lee did some admirable work. *Ars Technica* commented that "The crowning achievement came Thursday as contestant JungHoon Lee, aka lokihardt, demonstrated an exploit that felled both the stable and beta versions of Chrome." Lee was the story of the hour, the story of the Day 2. While no browser security will always stay perfect, Chrome generally is known as the browser which is especially tough to crack. *TechCrunch* commented that the browser bug found in Chrome resulted in the biggest payout in the contest's history. The amount was $110,000. JungHoon Lee, said the report, got $75k for the initial bug, $25k for getting his code to run at a system level, and another $10k because the bug worked in the beta build.

HP's contest is a win-win for those who do the exploits and for the vendors involved. The information goes right to the vendors so they can make their browsers more secure. The companies get a chance to patch things up. Microsoft, Google, Mozilla, Apple and Adobe are vendors involved in this year's event and, according to Steve Povolny in another HP security blog, "each vendor gets immediate face-to-face time with the exploit developers in order to start the process of building timely security fixes."

More information: — h30499.www3.hp.com/t5/HP-Secur … 6722204#.VQ6xuFXF_GO
— h30499.www3.hp.com/t5/HP-Secur … 6722884#.VQ6xuFXF_GP