Master of Pwn

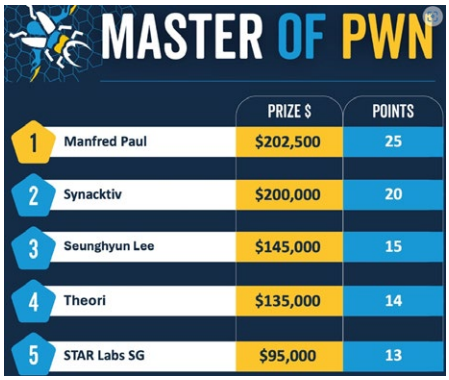
Wie findet man Sicherheitslücken in gleich vier Browsern, Manfred Paul?

Beim diesjährigen internationalen Hacker-Wettbewerb Pwn2Own hat Manfred Paul den ersten Platz belegt. Er schaffte es nicht nur, die Webbrowser Safari, Chrome und Edge zu hacken, sondern auch die Sandbox von Mozillas Firefox. Wir haben mit ihm über seine Motivation und sein Vorgehen gesprochen.

Von Marie-Claire Koch

c't: Herr Paul, Sie haben Sicherheitslücken in Edge, Chrome, Safari und Firefox entdeckt und auch gleich Wege gefunden, sie auszunutzen. Wie viel Zeit haben Sie dafür investiert?

Manfred Paul: Schwer zu sagen. Das ist von Target zu Target unterschiedlich. Am meisten Zeit verwende ich darauf, Dinge zu suchen und nichts zu finden. Verschwendet ist die Zeit aber nicht. Man lernt dazu und versteht Dinge, die dabei helfen können, später vielleicht doch etwas zu finden. Es ist aber zu einem gewissen Grad auch Glückssache.



Manfred Paul hat Sicherheitslücken in vier großen Browsern gefunden und beim diesjährigen Pwn2Own-Hacking-Wettbewerb den ersten Platz erreicht.

c't: Was dauert länger, eine Lücke zu finden oder sie auszunutzen?

Paul: Das ist verschieden. Für mich nimmt auf jeden Fall das Bug-Suchen den Großteil der Zeit in Anspruch. Es kommt auf die Methode an. Ich schaue mir oft den Code an und versuche auf diese Weise, Bugs zu finden. Aber das ist nur meine bevorzugte Arbeitsweise. Andere arbeiten mehr mit automatischen Tools. Die zum Laufen zu bringen kostet aber auch Zeit. Natürlich geht es schneller, wenn man schon Erfahrung hat.

c't: Haben Sie ein Rezept, nach dem Sie vorgehen?

Paul: Es ist viel Intuition dabei. Ich schaue mir tendenziell die Teile vom Code an, bei denen ich denke: „Wenn ich da etwas finde, dann ist das schwerwiegend". Ich achte stark auf den Just-in-Time-Compiler, also auf Code, der zur Laufzeit neuen, optimierten Maschinencode erzeugt.

c't: Wie sieht Ihre Vorarbeit aus?

Paul: Da bin ich eher unorganisiert. Andere gehen strukturierter vor und lesen etwa vergangene Exploits nach. Ich will lieber unbefangener an die Sache herangehen. Wenn ich weiß, was schon alles gefunden wurde, habe ich das Gefühl, „Der Code wird jetzt schon irgendwie seine Richtigkeit haben". Dann kann ich mich nicht mehr kritisch damit auseinandersetzen.

c't: Gibt es einen Exploit, auf den Sie besonders stolz sind?

Paul: Alle hatten ihre Herausforderungen. Firefox war der einzige Browser, bei dem ich auch die große Sandbox angegriffen habe. Die bietet zusätzlichen Schutz, den mein Exploit ausgehebelt hat, was ihn auch gerade für Endnutzer relevant macht.

c't: Sie haben mit Ihrer Arbeit mal eben Millionen Euro verbrannt. Was ist Ihre Motivation dafür?

Paul: Ich weiß, ich könnte mehr Geld verdienen, wenn ich meine Funde an den Höchstbietenden verkaufen würde. Aber ich will nicht dafür verantwortlich sein, dass Angreifer Schaden anrichten. Daher freut es mich auch wirklich, wenn Lücken anschließend gepatcht werden. Software sollte für alle sicher sein. Zum Beispiel die Firefox-Schwachstelle wurde im Rekordtempo beseitigt und das Update kam schnell heraus.

c't: Wie kamen Sie zur IT-Sicherheit?

Paul: Mein Einstieg in das Thema IT-Security waren sogenannte Capture-the-Flag-Wettbewerbe. Das sind Hacking-Turniere, bei denen man im Code einer Software absichtlich versteckte Bugs finden soll. Dabei habe ich viel gelernt. Ich habe ein Team, mit dem ich immer noch gelegentlich spiele. Nützlich war auch mein Mathematikstudium. Es macht sich vor allem in meiner Methodik bemerkbar: Ich versuche oft, quasi mental einen Beweis zu finden, dass Software korrekt ist.

c't: Obwohl Experten es fordern, wurde der Hackerparagraf bisher nicht abgeschafft. Hatten Sie zu Beginn Ihrer Laufbahn Sorge, mit dem Gesetz in Konflikt zu kommen?

Paul: Da gibt es eine große Schieflage, was die Gesetze angeht. Für die IT-Security-Community ist es eine Schande, zu sehen, dass vor Kurzem wieder jemand verurteilt wurde [1], der eine Sicherheitslücke gemeldet hatte. Ich hoffe, dass sich die Gesetzeslage ändert, damit man rechtssicher Lücken melden kann.

Auch das Thema „Reverse Engineering" ist in Deutschland rechtlich schwierig. Da kann man als Sicherheitsforscher schon einmal mit dem Urheberrecht in Konflikt kommen. Für mich bestand bisher weniger die Gefahr, weil ich mich primär mit Open-Source-Software beschäftigt habe. Meine ersten Sicherheitslücken habe ich im Linux-Kernel gefunden. Das ist ja keine Infrastruktur, die jemandem gehört. *(kst@ct.de)* c't

Literatur

[1] Sylvester Tremmel, Unversehens kriminell, „Hackerparagrafen" und warum sie problematisch sind c't 5/2024, S. 32

Pwn2Own-Website, weitere Berichterstattung: ***ct.de/y64t***