Wettbewerb um selbstheilende Software

Dieses Jahr gehen auf der Cyber Grand Challenge erstmals Computer statt Hacker autark auf Bug-Jagd und versuchen auch, Lücken abzusichern.

Auf der diesjährigen Hacker-Veranstaltung Def Con ruft die Defense Advanced Research Projects Agency (DARPA) sieben vorausgewählte Teams dazu auf, fortschrittliche Sicherheitsprogramme zu entwickeln und in der Praxis gegeneinander antreten zu lassen. Die Software muss nicht nur automatisch und autark Sicherheitslücken finden, sondern diese auch patchen.

Die Ergebnisse sollen als Basis für die Entwicklung von sich selbstheilender Software dienen. Offensichtlich ist das der DARPA viel Geld wert: Eigenen Angaben zufolge hat sie 55 Millionen US-Dollar in den diesjährigen Wettbewerb investiert. Das Event findet am 4. August in Las Vegas statt. Wer möchte, kann die sogenannte Cyber Grand Challenge im Live-Stream ab acht Uhr morgens deutscher Zeit verfolgen; und das könnte richtig spannend werden.

Die DARPA inszeniert den Hacking-Wettbewerb als klassisches Capture-the-Flag-Event. Dabei analysieren aber nicht die Hacker Software auf Schwachstellen und implementieren Fixes: Bei der diesjährigen Cyber Grand Challenge stehen erstmals Computer im Rampenlicht und treten gegeneinander an. Diese müssen automatisch und ohne menschliches Eingreifen in der Lage sein, Lücken im von der DARPA vorgegebenen Code zu erkennen und so schnell wie möglich abzusichern. Der Wettbewerb läuft zehn Stunden.

Was abstrakt klingt, sollen Live-Animationen für die Zuschauer veranschaulichen und verständlich machen. In der Arena zeigen sieben große Bildschirme jeweils den aktuellen Status eines Teams an. Dabei repräsentieren Sechsecke mögliche Angriffspunkte. Stößt die Software eines Teams auf eine Lücke und beginnt mit der Heilung, schießt der Code in Form eines Pixel-Strahls auf den jeweiligen Punkt – Tron lässt grüßen. Damit man als Zuschauer in dem Gewusel nicht den Überblick verliert, ist jedem Team eine Farbe zugeteilt. Schließt ein Team eine Lücke erfolgreich, wird diese entsprechend eingefärbt. Zudem sollen Moderatoren das Geschehen verständlich kommentieren. Insgesamt winken vier Millionen US-Dollar Preisgeld. Damit vom Wettstreit auch langfristig etwas übrig bleibt, will die DARPA den Code der Wettbewerbsteilnehmer als Open Source veröffentlichen. *(des@ct.de)*

BIOS-Lücke betrifft fünf Computer-Hersteller

Die vom Sicherheitsforscher Dmytro Oleksiuk entdeckte und mit dem Namen ThinkPwn getaufte BIOS-Lücke gefährdet diverse Computer-Modelle von Dell, Fujitsu, Gigabyte, HP und Lenovo. Der Name der Lücke rührt daher, dass Oleksiuk zuerst bei seinem ThinkPad auf die Schwachstelle gestoßen ist.

Angreifer können über die BIOS-Lücke im System Management Mode (SMM) Code am Betriebssystem vorbei ausführen und direkt auf Hardware-Komponenten zugreifen. Dafür müssen sie aber über lokale Admin-Rechte verfügen. In dieser Position kontrollieren Angreifer schon per se ein System. Über die Lücke können sie sich aber quasi unsichtbar und vor allem so einnisten, dass eine Reinigung im Grunde unmöglich ist.

So ließe sich etwa der Schreibschutz der Firmware aushebeln, um ein BIOS-Rootkit zu installieren. Angreifer könnten via ThinPwn auch den hochsicheren Credential Guard von Windows 10 aufbrechen, um Passwörter zu klauen. Auf den Credential Guard kann sonst nur privilegierte System-Software zugreifen.

Besitzer eines gefährdeten Computers müssen aber nicht in Panik verfallen: Der Exploit von Oleksiuk funktioniert nur von einem USB-Stick. Ein Angreifer müsste also Zugang zum Computer eines potenziellen Opfers haben und wie beschrieben über Admin-Rechte verfügen. Oleksiuk relativiert mögliche Angriffe weiter: „Es ist sehr unwahrscheinlich, dass die Schwäche in freier Wildbahn ausgenutzt wird."

Lenovo hat mittlerweile eine umfangreiche Liste mit betroffenen und nicht betroffenen Geräten veröffentlicht (siehe c't-Link). Daraus kann man auch entnehmen, wann abgesicherte BIOS-Updates erscheinen sollen. Die Veröffentlichungszeiträume sind weit gestreut: Einige Aktualisierungen verspricht der Hersteller für Ende Juli; andere Geräte können Besitzer den Angaben zufolge erst Ende September absichern. Statements von weiteren Herstellern stehen noch aus.

(des@ct.de)

Sicherheits-Notizen

Die Entwickler des **Foxit Reader** und **Phantom** schließen in neuen Versionen acht kritische Sicherheitslücken.

Der **Facebook Messenger** verschickt Nachrichten optional Ende-zu-Ende-verschlüsselt. Die Funktion ist derzeit im Testbetrieb; im Sommer sollen alle davon profitieren.

D-Link hat für verschiedene Produkte (siehe c't-Link), darunter etwa NAS-Geräte und Webcams, Sicherheits-Updates zum Download bereitgestellt.

Wer das Plug-in **All in One SEO** für seine WordPress-Seite nutzt, sollte zügig die abgesicherte Version 2.3.8 einspielen, da Angreifer im schlimmsten Fall Admin-Sessions übernehmen könnten.

In den optionalen Modulen Coder, RESTWS und Webform Multiple File Upload für **Drupal** klaffen kritische Lücken. Updates sind verfügbar.