COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/angreifbare-sicherheitsluecken-in-intels-vpro,1883420

Hacker sagen

Angreifbare Sicherheitslücken in Intels vPro

Datum: 08.01.2009
Autor(en): Uli Ries

IT-Sicherheitsexperten haben Intels Management-Technik vPro gehackt. Sie wollen eine Lücke gefunden haben, durch die sich Intels TXT (Trusted Execution Technology) umgehen lässt. Eigentlich soll TXT Programme vor schädlichen Manipulationen schützen. Die Hacker wollen die Wirksamkeit ihrer Entdeckung in Kürze öffentlich präsentieren.

Am Werk: Intel ist dabei, das Sicherheitsproblem in vPro zu beheben.

Joanna Rutkowska und Rafal Wojtczuk von **Invisible Things Labs**[1] wollen auf der kommenden IT-Sicherheitskonferenz **Black Hat**[2] (16. bis 19. Februar, Washington, USA) demonstrieren, dass sie **Intels TXT**[3] umgehen können und Anwendungen trotz deren Vertrauen auf TXT manipulieren können. Genau das soll TXT, das integraler Bestandteil von **Intels**[4] Management-Plattform **vPro**[5] ist, aber verhindern. TXT wurde konzipiert, um beispielsweise Anwendungen, die in einer virtuellen Maschine laufen, von anderen auf dem gleichen System ausgeführten – möglicherweise schädlichen – Programmen zu trennen. Oder um vollständige Betriebssysteme sowie Hypervisor sicher und ohne Modifikationen durch Malware starten zu können, selbst wenn das System beispielsweise durch Bios-Viren verseucht ist.

Die Hacker haben funktionierenden Proof-of-Concept-Code erstellt, der eine Attacke auf tboot, Intels Implementierung des sicheren Bootvorgangs von **Xen**[6] und **Linux**[7], demonstrieren soll. Rutkowska, bisher hauptsächlich durch ihre **Hypervisor-Angriffe**[8] bekannt geworden, und ihr Kollege Wojtczuk schreiben, dass sie eine zweistufige Attacke konzipiert haben. Zu erst nutzen sie einen Bug in Intels Systemsoftware aus. Der zweite Schritt baut auf einem Designfehler in TXT selbst auf. Mehr Details über den Bug und die angegriffene Software verraten die Experten vorerst nicht, um böswilligen **Hackern**[9] keine Anhaltspunkte zu liefern.

Die Hacker haben Intel im Dezember 2008 auf die Probleme hingewiesen und der Hersteller arbeitet an momentan an einer Lösung des Sicherheitsproblems. Laut Invisible Things Labs hat **Intel**[10] zugesagt, Entwicklern eine verbesserte TXT-Spezifikation zur Verfügung zu stellen. Diese neue Spezifikation soll erklären, wie TXT-Loader abgesichert werden können.

Noch wird TXT kaum eingesetzt, da die Technik erst seit einem knappen Jahr verfügbar ist. Der Xen-Hypervisor dürfte die momentan prominenteste Anwendung sein, die sich beim Starten auf die Absicherung durch TXT verlässt. Nachdem TXT laut Rutkowska aber großes Potential hat und viele der heute bekannten Sicherheitsprobleme beheben könnte, könnte ein in Zukunft erfolgreich ausgeführter Angriff fatale Folgen für die Sicherheit großer Netzwerke haben.

Links im Artikel:

[1] **http://www.invisiblethingslabs.com/**
[2] **http://www.blackhat.com/**

[3] **http://www.intel.com/technology/security/**
[4] **https://www.computerwoche.de/schwerpunkt/i/Intel.html**
[5] **http://www.intel.com/technology/vpro/index.htm**
[6] **http://www.xen.org/**
[7] **https://www.computerwoche.de/schwerpunkt/l/Linux.html**
[8] **https://www.computerwoche.de/knowledge_center/security/1863677/**
[9] **https://www.computerwoche.de/schwerpunkt/h/Hacker.html**
[10] **http://de.wikipedia.org/wiki/Intel**
