CYBERUS
TECHNOLOGY

Cyberus Technology GmbH · Geibelstr. 15 · 01139 Dresden

Telefon +49 175 431 66 77
service@cyberus-technology.de

www.cyberus-technology.de

Schwere Sicherheitslücke in Intel Prozessoren

Experten von Cyberus Technology versetzen die Computerwelt in Aufregung

Dresden - Am 3. Januar 2018 wurden gravierende Schwachstellen moderner Prozessoren publik, die zu den größten Sicherheitslücken der vergangenen Jahre führen. Zu den Entdeckern gehören dabei auch IT-Spezialisten des Dresdner Start-Ups Cyberus Technology. Das besondere dabei: die Ursache ist direkt in den Computerchips zu suchen, d.h. alle Anwender sind, unabhängig von der verwendeten Software, betroffen.

Gegen Jahresende fing die Gerüchteküche im Internet zu brodeln an und es mehrten sich die Hinweise auf massive Sicherheitsprobleme. Bereits am 1. Dezember hatten Thomas Prescher und Werner Haas den Chipgiganten Intel auf Probleme mit seinen Prozessoren hingewiesen. Die Information wurde jedoch unter Verschluss gehalten, um zeitgleich mit der Veröffentlichung Gegenmaßnahmen zur Hand zu haben. In der Zwischenzeit bildete sich ein internationales, 10-köpfiges Team aus Forschern, die unabhängig voneinander ähnliche Ergebnisse erzielt hatten.

Es stellte sich heraus, dass eine ganze Klasse neuartiger Angriffsvektoren entdeckt wurde, deren beiden Hauptvarianten auf die Namen Meltdown bzw. Spectre getauft wurden. Außerdem wurde offensichtlich, dass nicht nur Intel-Produkte sondern alle Hersteller betroffen waren. Schließlich ist die Ursache in einem Grundprinzip moderner Hochleistungsprozessoren zu suchen: um unproduktive Wartezeiten zu minimieren wird mit der Abarbeitung neuer Befehle bereits begonnen wenn die Ergebnisse vorangegangener Instruktionen noch nicht vollständig bekannt sind. Dieses Verfahren wird mit spekulativer Ausführung bezeichnet. Dabei erkennt und korrigiert ein Prozessor etwaige Fehler. Die bahnbrechende Erkenntnis der Forscher: Angreifer können einen Prozessor gezielt auf eine falsche Fährte locken und trotz der Fehlerkorrektur Spuren der spekulativen Aktionen erkennen. Durch geschickte Irreführung ist es dann möglich an Daten zu gelangen, die vor unzulässigen Zugriffen bei normaler Programmausführung geschützt sind.

Cyberus Technology ist ein Start-Up Unternehmen mit Fokus auf Cyber-Sicherheit. Die Firmengründer können dabei auf mehr als 50 Jahre Berufserfahrung u.a. bei Intel USA, im Germany Microprocessor Lab oder dem Sicherheitsspezialisten FireEye zurückblicken. Neben Software zur Analyse von Schadprogrammen bildet der Schutz kritischer Systemkomponenten einen weiteren Schwerpunkt der Entwicklungsarbeit. Inzwischen wurden die Geschäftspartner über die neuen Angriffsmöglichkeiten informiert und Experten stehen auf Anfrage für detaillierte Beratung zur Verfügung.

Weitere Informationen zum Thema:

- https://meltdownattack.com/
- https://blog.cyberus-technology.de/posts/2018-01-03-meltdown.html