Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Neue Sicherheitslücke bei Intel-Prozessoren entdeckt

Hersteller reagiert auf Hinweis der TU Darmstadt / Schwachstelle behoben

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihre Ansprechpartnerin:
Silke Paradowski
Tel. 06151 16 - 20019
Fax 06151 16 - 23750
silke.paradowski@tu-darmstadt.de

www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Darmstadt, 13. Dezember 2019. Ein Team der TU Darmstadt hat unter der Leitung von Professor Ahmad-Reza Sadeghi einen neuen gravierenden Angriff, „V0LTpwn“, auf Intel-Prozessoren veröffentlicht. Das Unternehmen hat die Sicherheitslücke nach Hinweis der TU geschlossen.

In den vergangenen Jahren wurden immer wieder verheerende Schwachstellen in Prozessoren, den Herzstücken von Computern, entdeckt. Einige der neuesten Beispiele für Sicherheitslücken in Prozessoren sind „Meltdown“, „Spectre“ und „Foreshadow“. Diese Angriffe nutzen Design- und Implementierungsfehler von Optimierungsverfahren zur Beschleunigung der Prozessorberechnungen aus, um geheime Informationen, wie kryptografische Schlüssel, auszulesen.
Forscher des System Security Lab der TU Darmstadt haben unter der Leitung von Professor Ahmad-Reza Sadeghi nun einen neuartigen gravierenden Angriff, „V0LTpwn“, auf Intel-Prozessoren veröffentlicht. Im Gegensatz zu bisherigen Angriffen ermöglicht „V0LTpwn“ die direkte Manipulation der CPU-Berechnungen. Der Angreifer kann beispielsweise kryptographische Operationen manipulieren und somit falsche Berechnungsergebnisse provozieren.
„V0LTpwn“ nutzt einen völlig neuen Ansatz, nämlich die Herabsenkung der Prozessor-Spannung auf eine kritische Schwelle, ab der bestimmte Instruktionen nicht mehr korrekt funktionieren und Fehler produzieren. Das Team der TU konnte mit einem Angriff zeigen, wie sogar die Ausführung von Software-Programmen beeinflusst werden kann, sofern darin anfällige Instruktionen enthalten sind.
Für ihren Angriff nutzten die Darmstäter Forscher eine Software-Schnittstelle in Intel-Prozessoren, die zum Beispiel von Gamern beim sogenannten „Übertakten“ ihrer Prozessoren verwendet wird. Da für den Zugriff auf diese Schnittstellen erweiterte Systemrechte notwendig sind, stellt die Sicherheitslücke für gewöhnliche Anwender keine Gefahr dar. Obwohl dieser Angriff für alle gängigen Intel-Prozessoren anwendbar ist, betonen die Forscher, dass der eigentliche Angriff sich primär auf die neuesten Intel-SGX-Prozessoren richtet, die eine Reihe von modernen Sicherheitsfunktionen zum Schutz der Software bieten. Intel SGX ist erst seit 2015 in Intel-CPUs vorhanden.
In Rahmen eines Responsible Disclosure wurden die Ergebnisse zunächst vertraulich an Intel gemeldet. Intel hat bereits entsprechende

Sicherheitsmaßnahmen eingesetzt und stellt sie für alle betroffenen Plattformen bereit.
Seit 2012 gibt es ein gemeinsames Forschungslab von Intel und der TU Darmstadt.

Kontakt

Prof. Dr.-Ing. Ahmad-Reza Sadeghi
System Security Lab
Fachbereich Informatik
Tel.: 06151/16-25328
ahmad.sadeghi@trust.tu-darmstadt.de

Über die TU Darmstadt

Die TU Darmstadt zählt zu den führenden Technischen Universitäten in Deutschland. Sie verbindet vielfältige Wissenschaftskulturen zu einem charakteristischen Profil. Ingenieur- und Naturwissenschaften bilden den Schwerpunkt und kooperieren eng mit prägnanten Geistes- und Sozialwissenschaften. Weltweit stehen wir für herausragende Forschung in unseren hoch relevanten und fokussierten Profilbereichen: Cybersecurity, Internet und Digitalisierung, Kernphysik, Energiesysteme, Strömungsdynamik und Wärme- und Stofftransport, Neue Materialien für Produktinnovationen. Wir entwickeln unser Portfolio in Forschung und Lehre, Innovation und Transfer dynamisch, um der Gesellschaft kontinuierlich wichtige Zukunftschancen zu eröffnen. Daran arbeiten unsere 308 Professorinnen und Professoren, 4.500 wissenschaftlichen und administrativ-technischen Mitarbeiterinnen und Mitarbeiter sowie rund 25.200 Studierenden. Mit der Goethe-Universität Frankfurt und der Johannes Gutenberg-Universität Mainz bildet die TU Darmstadt die strategische Allianz der Rhein-Main-Universitäten.

www.tu-darmstadt.de

MI-Nr. 87/2019, Kenjar/Braun/sip