idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Eidgenössische Technische Hochschule Zürich (ETH Zürich)
Franziska Schmid
05/13/2025
http://idw-online.de/en/news852030

Research projects, Research results
Electrical engineering, Information technology
transregional, national

ETH-Forschende finden neue Sicherheitslücke in Intel-Prozessoren

ETH-Informatiker haben eine neue Klasse von Schwachstellen in Intel-Prozessoren gefunden. Über sorgfältig ausgearbeitete Befehlsabfolgen können sie die Barrieren zwischen den Prozessor-Nutzenden durchbrechen. Mit schneller Angriffswiederholung lässt sich der ganze Prozessorspeicher lesen.

Wer im Vorfeld auf wahrscheinliche Ereignisse spekuliert und sich dementsprechend vorbereitet, kann schneller auf neue Entwicklungen reagieren. Was praktisch jeder Mensch bewusst oder unbewusst tagtäglich praktiziert, nutzen auch moderne Computer-Prozessoren, um den Ablauf von Programmen zu beschleunigen. Sie verfügen über sogenannt spekulative Technologien, mit denen Sie beispielsweise Anweisungen auf Reserve ausführen, die aus Erfahrung als nächste kommen dürften. Durch diese Vorwegnahme einzelner Rechenschritte wird die Informationsverarbeitung insgesamt beschleunigt.

Was im Normalbetrieb die Computer-Leistung steigert, kann aber auch zu einer Hintertüre für Hacker werden, wie eine aktuelle Forschungsarbeit von Informatikern der Computer Security Group (COMSEC) am Departement für Informationstechnologie und Elektrotechnik der ETH Zürich zeigt. Die Computerwissenschaftler haben eine neue Klasse von Schwachstellen gefunden, mit denen die Vorhersage-Berechnungen der sogenannten CPU (Central Processing Unit) missbraucht werden können, um unberechtigt an Informationen von anderen Prozessor-Nutzer:innen zu gelangen.

PC-, Laptop- und Server-Prozessoren betroffen

«Die Sicherheitslücke öffnet sich in allen Intel-Prozessoren», betont Kaveh Razavi, der Leiter der COMSEC: «Wir können über die Schwachstelle die Inhalte des Puffer-Speichers des Prozessors (Cache) und des Arbeitsspeichers (RAM) eines anderen Nutzers der gleichen CPU vollständig auslesen.» Die CPU verwendet den RAM-Speicher (Random-access Memory) und den Cache-Speicher zur temporären Zwischenspeicherung von Berechnungsschritten und von den wahrscheinlich als nächstes benötigten Informationen.

Die Lücke untergräbt insbesondere im Cloud-Umfeld, in dem sich viele Nutzer:innen die gleichen Hardware-Ressourcen teilen, die Datensicherheit grundlegend. Betroffen sind sowohl die Prozessoren des weltweit grössten CPU-Herstellers, die in PCs und Laptops arbeiten als auch diejenigen, die in Rechenzentrums-Servern zum Einsatz kommen.

Nanosekunden-Lücke in der Berechtigungsüberprüfung

Die sogenannten BPRC (Branch Predictor Race Conditions) entstehen jeweils während einer kurzen Zeitspanne von wenigen Nanosekunden, wenn der Prozessor zwischen Vorhersageberechnungen für zwei Anwender:innen mit unterschiedlichen Berechtigungen wechselt, erklärt Sandro Rüegge, der die Schwachstelle in den letzten Monaten genauer unter die Lupe genommen hat.
Das Durchbrechen der eingebauten Schutzbarrieren zwischen den Nutzer:innen, den sogenannten Privilegien, wird möglich, weil das Abspeichern der Berechtigungen der einzelnen Aktivitäten nicht gleichzeitig mit den Berechnungen

erfolgt. Mit speziellen Eingaben kann nun bei einem Anwender:innen-Wechsel eine Uneindeutigkeit in der Reihenfolge der Ereignisse provoziert werden und es kommt zu einer falschen Zuordnung der Privilegien. Dies kann eine Angreifer:in nutzen, um ein Informations-Byte (Einheit aus acht binären 0/1-Informationen) auszulesen.

Byte für Byte zum ganzen Speicherinhalt

Die Offenlegung eines einzelnen Bytes wäre vernachlässigbar. Der Angriff lässt sich aber in schneller Abfolge wiederholen, und so können mit der Zeit die ganzen Speicherinhalte ausgelesen werden, verdeutlicht Rüegge. «Wir können den Fehler andauernd gezielt auslösen und dadurch eine Auslesegeschwindigkeit von über 5000 Byte pro Sekunde erreichen.» Im Fall eines Angriffs ist es also nur eine Frage der Zeit, bis die Informationen der gesamten CPU-Speicher in die falschen Hände geraten.

Teil einer Serie von Sicherheitslücken

Die Schwachstelle, die die ETH-Forscher jetzt gefunden haben, ist nicht die erste, die in den –Mitte der 1990er-Jahre eingeführten – spekulativen CPU-Technologien entdeckt wurde. 2017 machten mit Spectre und Meltdown die ersten zwei Schwachstellen dieser Art Schlagzeilen und seither kommen regelmässig neue Varianten hinzu. Johannes Wikner, ein ehemaliger Doktorand in Razavis Gruppe, identifizierte bereits 2022 eine als Retbleed bezeichnete Sicherheitslücke. Er nutzte dabei Spuren von spekulativ ausgeführten Anweisungen in den Zwischenspeichern der CPU, um an Informationen von anderen Nutzer:innen zu gelangen.

Verdächtiges Signal entlarvt die Lücke

Den Ausgangpunkt für die Entdeckung der neuen Schwachstellen-Klasse bildeten Arbeiten im Anschluss an die Retbleed-Untersuchungen. «Ich untersuchte die Funktionen der Schutzmassnahmen, die Intel zur Absicherung der Lücke eingeführt hatte», sagt Johannes Wikner. Dabei entdeckte er ein ungewöhnliches Signal des Cache-Speichers, das unabhängig davon auftauchte, ob die Schutzmassnahmen ein- oder ausgeschaltet waren. Rüegge übernahm darauf die genauere Analyse der Signalursache und konnte darauf aufbauend den neuen Angriffsweg enthüllen.

Grundlegendes Architekturproblem

Entdeckt wurde die Lücke bereits im September 2024. Seither hat Intel die Schutzmassnahmen zur Absicherung der Prozessoren umgesetzt. Dennoch deutet vieles auf ein schwerwiegenderes Problem hin. «Die Serie von neuentdeckten Lücken in den spekulativen Technologien ist ein Hinweis auf grundlegende Fehler in der Architektur», gibt Razavi zu bedenken: «Die Lücken müssen eine nach der anderen gefunden und dann geschlossen werden.»
Um derartige Lücken zu schliessen, ist eine spezielle Aktualisierung im sogenannten Mikrocode des Prozessors nötig. Diese kann über ein BIOS- oder ein Betriebssystem-Update erfolgen und dürfte darum in einem der aktuellen «kumulativen Updates» von Windows auf unseren PCs installiert werden.

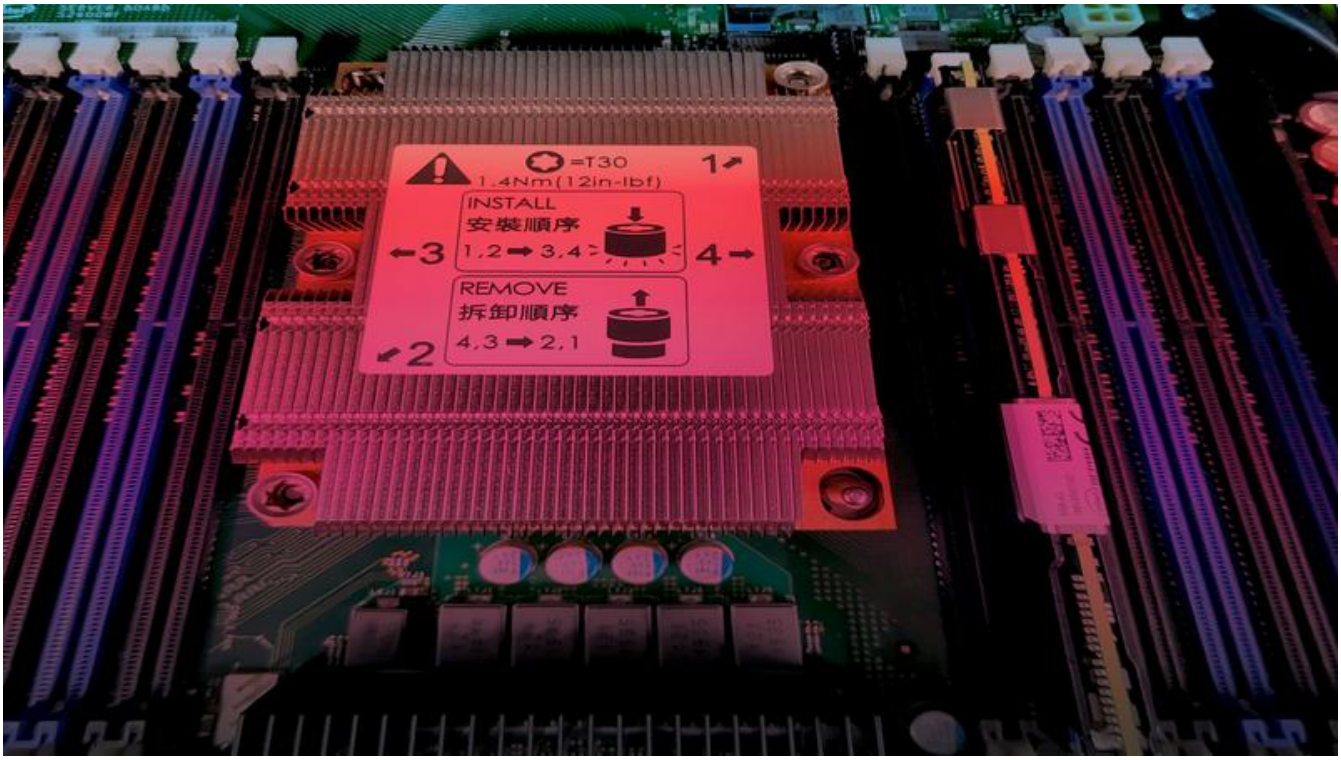
contact for scientific information:
Prof. Dr. Kaveh Razavi, ETH Zürich, kaveh(at)ethz.ch

Original publication:

Rüegge S, Wikner, J, Razavi, K. Branch Privilege Injection: Compromising Spectre v2 Hardware Mitigations by Exploiting Branch Predictor Race Conditions. 34th USENIX Security Symposium, 2025.
CVE-Nummer: CVE-2024-45332

URL for press release: https://comsec.ethz.ch/bprc

URL for press release: https://ethz.ch/de/news-und-veranstaltungen/eth-news/news/2025/05/eth-forschende-finden-neue-sicherheitsluecke-in-intel-prozessoren.html



Alle Intel-Prozessoren ab 2018 sind von der Sicherheitslücke «Branch Privilege Injection» betroffen. Das Bild zeigt das Beispiel eines Intel-Server-Systems.
Computer Security Group
Hochschulkommunikation, ETH Zürich