Side-Channel-Attacks auf Pipelining - ACOnet-CERT-Aussendung

Sobald der Wissernsstand.etwas gesettlet erschien und wir uns einen Überblick über die Thematik verschafft hatten, haben wir die ACOnet-Constituency mit folgendem Text informiert:

Liebe Kolleg/inn/en,

es gibt viel medial unterstützte Aufregung rund um "den Intel-Bug", aber diesmal ist das Problem real und ernstzunehmen.

Es gibt noch wenig belastbare und hilfreiche Informationen. Hier unser aktueller Stand dazu und eine Anregung für die Kommunikation mit den UserInnen.

Worum geht es?

Es handelt sich um ein neuartiges Szenario, das nahezu alle modernen Microprozessoren betrifft, und dessen Auswirkungen noch nicht vollständig erforscht sind.

Die bekanntgewordenen Exploits Meltdown und Spectre nutzen Unterschiede im Timing-Verhalten des Systems, die durch Inhalte von im Programmiermodell nicht zugänglichem Speicher entstehen.

Hier handelt es sich nicht um eine singuläre Sicherheitslücke, sondern um eine völlig neue Angriffsmethode auf grundlegende Optimierungsfeatures (Pipelining) von CPU-Architekturen im Allgemeinen. Es ist daher zu befürchten, dass noch weitere Entdeckungen in diesem Themenkreis folgen werden; wir sehen möglicherweise erst die Spitze eines Eisbergs.

Auswirkungen

Durch den Zugriff auf Speicherbereiche, die ansich nicht gelesen werden können, kann ein Angreifer am Hardwareschutz vorbei Informationen auch von anderen Prozessen oder dem Betriebssystem auslesen.

Besondere Vorsicht ist bei Multi-User-Systemen, virtuellen Umgebungen etc. (lies: Cloud!) geboten, wo Executables von verschiedenen Anwendern auf der selben Hardware ausgeführt werden.

Unter Umständen können auch Script-Sprachen als Vektor dienen (Just In Time-Compiler). Daher sind auch z.B. Web-Browser am PC ein mögliches Einfallstor.

Auch ARM-Prozessoren sind in dieser Hinsicht modern. Daher sind auch mobile devices prinzipiell betroffen.

Zwar sind zur Zeit außer den bekannten PoC-Exploits keine Angriffe "in the wild" bekanntgeworden. Dies kann sich aber jederzeit ändern, u.U. auch mit einem abgewandelten Angriffspfad.

Was ist zu tun?

Das ursächliche Problem lässt sich derzeit nicht beheben, da es an der Hardware der CPU, eigentlich sogar an deren grundlegendem Design, liegt. Ob bzw. inwieweit Microcode-Updates wirksame Abhilfe schaffen können, ist momentan nicht bekannt.

Dennoch sind Softwareupdates zielführend und notwendig.

 * das Betriebssystem kann Microcode-Updates durchführen (auch ohne BIOS-Update)

 * das Betriebssystem kann mitigierende Maßnahmen setzen (z.B. Kaiser-Patch)

 * auch die Anwendungssoftware kann Angriffe erschweren (z.B. kein JIT in Firefox ESR, Site Isolation, ...)

Dass Maschinen und Software, die nicht mehr updatebar sind, dekommissioniert werden sollen, versteht sich ansich von selbst und wird durch die aktuelle Entwicklung erneut unterstrichen.

Im Übrigen bleibt die weitere Entwicklung, insbesondere was die Microcode-Updates betrifft, abzuwarten.

User-Kommunikation

Wir haben im Team überlegt, wie die nicht technisch orientierten AnwenderInnen zu informieren wären. Dabei ist zu berücksichtigen, dass es keine Lösung gibt, und reine Panikmache alles andere als hilfreich wäre. Als Anregung hier ein Vorschlag dazu:

"Titel: Umgang mit Meltdown, Spectre and more...

Bin ich betroffen?

Wahrscheinlich ja. Allerdings sind derzeit (noch) keine praktischen Angriffe bekannt.

Es handelt um sich um ein neuartiges Szenario das nahezu alle moderne Hardware betrifft und dessen Auswirkungen noch nicht vollständig erforscht sind.

Was ist zu tun?

Derzeit ist das ursächliche Problem nicht restlos behebbar. Durch aktualisierte Software kann aber die Angriffsfläche drastisch reduziert werden.

Die Software stets aktuell zu halten - auf PC ebenso wie auf Mobile Devices - ist daher wichtiger denn je:

http://zid.univie.ac.at/services/services-von-a-z/i/it-security/it-security-tipps/pc-software/

http://zid.univie.ac.at/services/services-von-a-z/i/it-security/it-security-tipps/fuer-eilige-5-security-tipps-fuer-mobilgeraete/Aktuell arbeiten Hard- und Software Hersteller an weiteren Lösungsansätzen."

Hoffe, das war eine nützliche Information -- Feedback ist wie immer gern gesehen.

Liebe Grüße vom ACOnet-CERT-Team!