Kwetsbaarheden in chips voor Laptops en Computer.

Afgelopen maand is bekendgemaakt dat er in Intel processoren een enorm lek zit, dat Meltdown heet. Er is nog een lek wat Spectre heet en in sommige processoren van AMD en ARM zit. Heel veel pc's en laptops en een aantal tablets en smartphones zijn daardoor kwetsbaar voor een of meer van deze lekken - waardoor privé-informatie uit het geheugen gestolen kan worden. Voor Windows, Mac en Linux en Android en iOS zijn er - gedeeltelijke - pleisters voor de lekken. Ook web browsers zijn kwetsbaar voor deze geheugenaanvallen.

Het Nationaal Cyber Security Center van het Ministerie van Justitie en Veiligheid (NCSC) draagt bij aan het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving door het leveren van inzicht en het bieden van handelingsperspectief.

Op de meeting van 3 maart heb ik geconstateerd dat er al verschillende laptops kwetsbaar hiervoor zijn. Ik heb een klein programmaatje hiervoor gebruikt waarin ik dat kon testen. Gelukkig zijn er bij DeCVB vooralsnog geen gevallen bekend van mensen die hierdoor zijn gehackt of gegevens zijn gestolen. Wel is het zo dat voor zowel bedrijven als thuisgebruikers gevoelige gegevens kunnen worden bemachtigd als ze hier geen maatregelen voor treffen. Het wil dus niet zeggen dat er geen misbruik zou kunnen plaatsvinden!
Daarom is het dus wel belangrijk updates uit te voeren en ontwikkelingen te volgen. Een aantal leveranciers, waaronder Microsoft en Mozilla, hebben patches aangekondigd of al beschikbaar gesteld. Om de kwetsbaarheden te mitigeren, zijn patches nodig van zowel software- als hardware leveranciers. Het is echter nog niet bekend of deze patches een deel van de kwetsbaarheden verhelpen of het volledige probleem wegnemen. Ook is niet bekend of dit in alle gevallen tot mogelijk verminderde prestaties kan leiden. Er is vooralsnog geen informatie die op actief misbruik wijst. Het detecteren van misbruik is echter complex en niet direct zichtbaar.
De verwachting is dat de groep van mogelijke aanvallers wel snel zal groeien nu volledige informatie over het onderzoek beschikbaar is. De gepubliceerde aanvalscode (PoC) kan immers worden hergebruikt door aanvallers. Maar het feit dat de PoC’s nu beschikbaar zijn, leidt niet direct tot verhoogd risico, omdat niet iedereen een dergelijk complexe aanval kan uitvoeren.

Meltdown heeft in het bijzonder impact op aanbieders van cloud - virtualisatiedienstverlening omdat het de onderlinge isolatie van virtuele systemen aantast. De aanval kan in dit geval komen vanuit een gebruiker van die systemen. Hierdoor kan de gebruiker toegang krijgen tot informatie uit het computergeheugen van andere gebruikers.

Met **Spectre** kunnen aanvallers informatie stelen uit een webbrowser, zoals cookies, TLS-sleutels en wachtwoorden. Een aanvaller die een slachtoffer kan verleiden een website te openen waarop de aanvaller malafide Javascript code heeft geplaatst, kan geheugen stelen dat toebehoort aan de webbrowser.

Er is een klein en handig programma om te controleren of je systeem kwetsbaar is voor Meltdown en Spectre en hier te vinden: https://www.grc.com/inspectre.htm

Informatie over deze meldingen staat ook hier beschreven: https://www.ncsc.nl/actueel/nieuwsberichten/meltdown-en-spectre.html en additionele informatie over Meltdown hier: https://meltdownattack.com/

Mocht je laptop of PC kwetsbaar zijn, ga dan naar de fabrikant van je laptop of zoek in het geval van een PC naar de fabrikant van je moederbord en zoek bij het model naar downloads of support. Kijk of er een nieuw BIOS update is.

Microsoft heeft aangegeven dat je met alleen updates voor Windows niet volledig beveiligd bent tegen de Meltdown- en Spectre-lekken. Je zult ook - door Intel en AMD gemaakte - firmware-updates voor je BIOS/UEFI moeten installeren **via je pc fabrikant** (bijvoorbeeld HP, Lenovo, Dell, Acer of ASUS).

Zelf heb ik mijn apparaten thuis al voorzien van updates. De meeste firmware-updates voor pc's (van niet ouder dan een jaar of vijf) **zijn in februari of maart of wellicht nog later uitkomen**. Afhankelijk van het merk of model zijn ze nog niet voor alle merken beschikbaar. Per fabrikant kan dit verschillen echter (bij samengestelde pc's kijk je naar de moederbord-fabrikant). De firmware updates zijn nodig voor Windows en Linux computers. Voor Mac-computers lijken ze vooralsnog niet nodig - of ze komen nog via Apple. Zie verder: https://www.gratissoftwaresite.nl/meltdown-spectre-lekken-intel-amd-arm-windows-mac-linux-android-patches#firmware