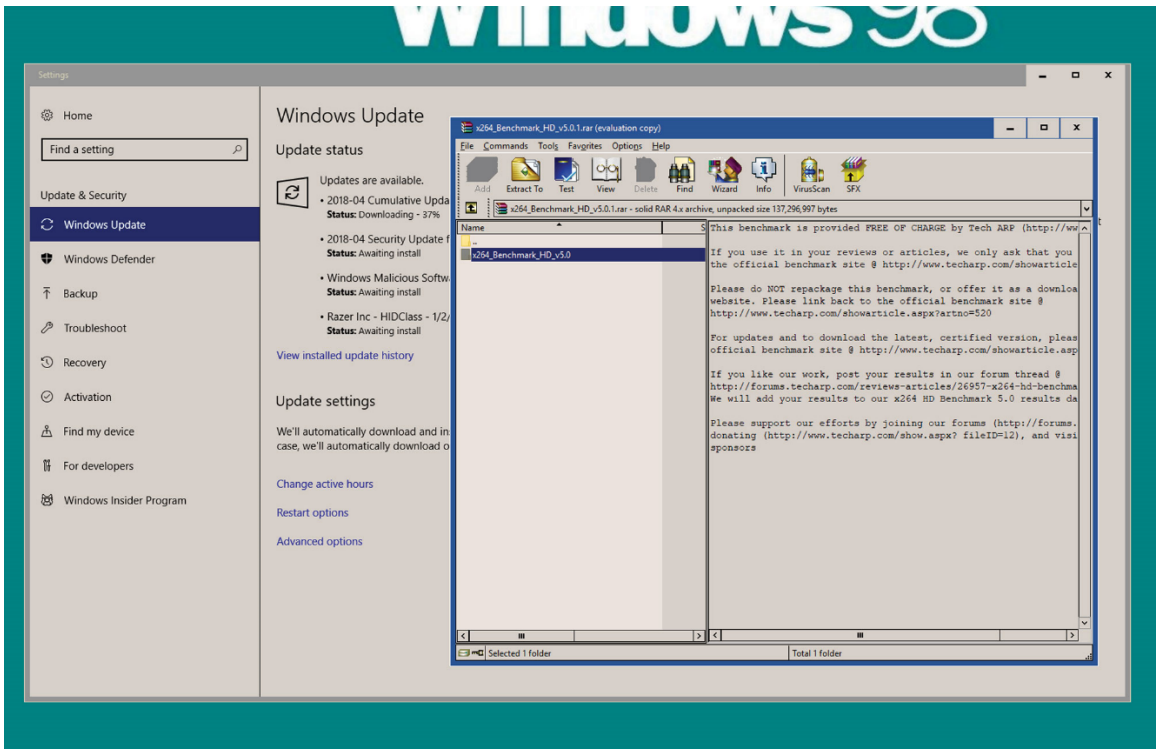


Guide: Reparer Windows med ét nemt værktøj

DE LYDER SOM EN BOND-FILM – OK FAKTISK VAR EN AF DEM EN BOND-FILM – MEN I SAMMENHÆNG MED COMPUTERE ER DER IKKE MEGET SJOV VED MELTDOWN OG SPECTRE

Randi | Zyberdata | 09-02-2019

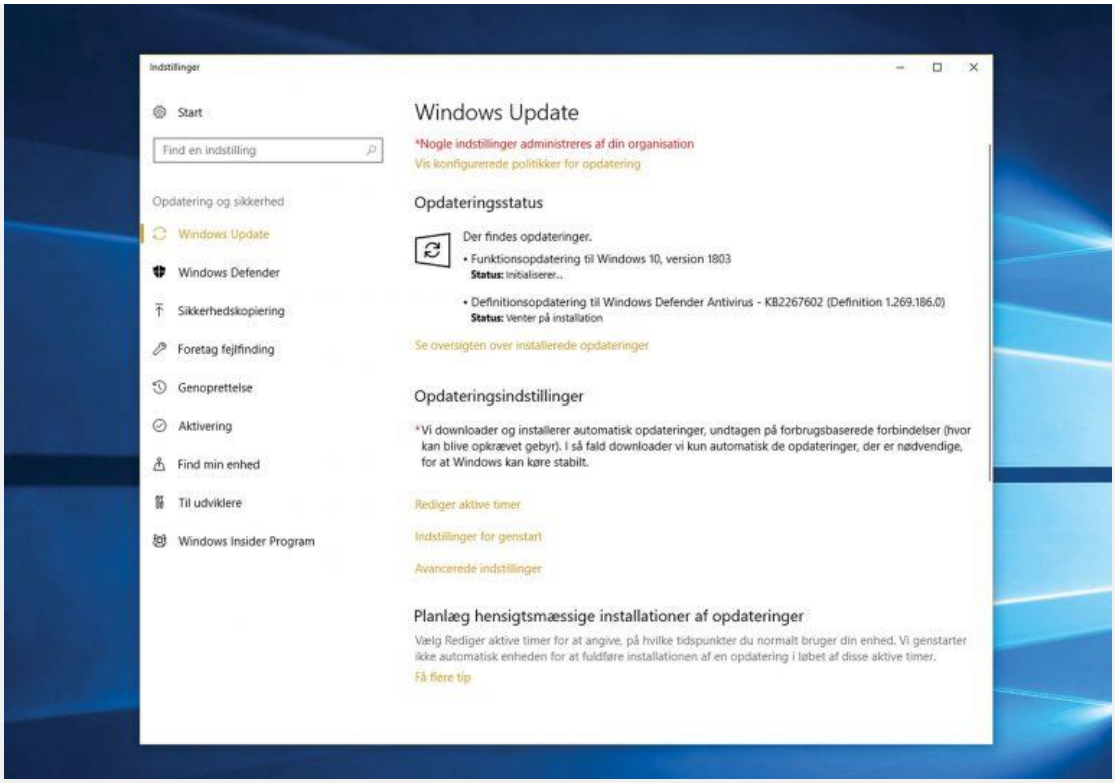
Meltdown og Spectre

Dette par, der udnytter kritiske sårbarheder i cpu'er, skabte megen tænders gnidsel i starten af 2018 på grund af hackeres mulighed for at ramme intet mindre end to årtiers processorer. Tænder blev skåret endnu mere, da der kom rapporter om, at Intel og AMD's fejlrettelse til sårbarhederne kunne få systemets ydelse til at falde.

Det vides dog ikke, hvor meget ydelsen kan falde, og det afhænger tildels af din cpu-model, dit OS, din lagerenhed og flere andre faktorer – og derfor er det tid til at rulle de metaforiske ærmer op og komme i gang med at teste. Ved at bruge en lille app, der slår Meltdown og Spectre-beskyttelsen til og fra ved at aktivere eller deaktivere deres associerede fixes og køre nogle cpu-benchmarks i begge miljøer, får du en forståelse for, hvor meget din ydelse eventuelt er faldet ved, at du holder dig beskyttet. Bemærk at vi ikke anbefaler, at du holder dine patches deaktiverede for at få ydelsen øget igen – hvad er lidt ydelse værd, hvis dine data er ubeskyttede? Dette er blot en øvelse for at se, om og hvor meget din ydelse har taget skade.

1 Tillad alle Meltdown og Spectre-opdateringer

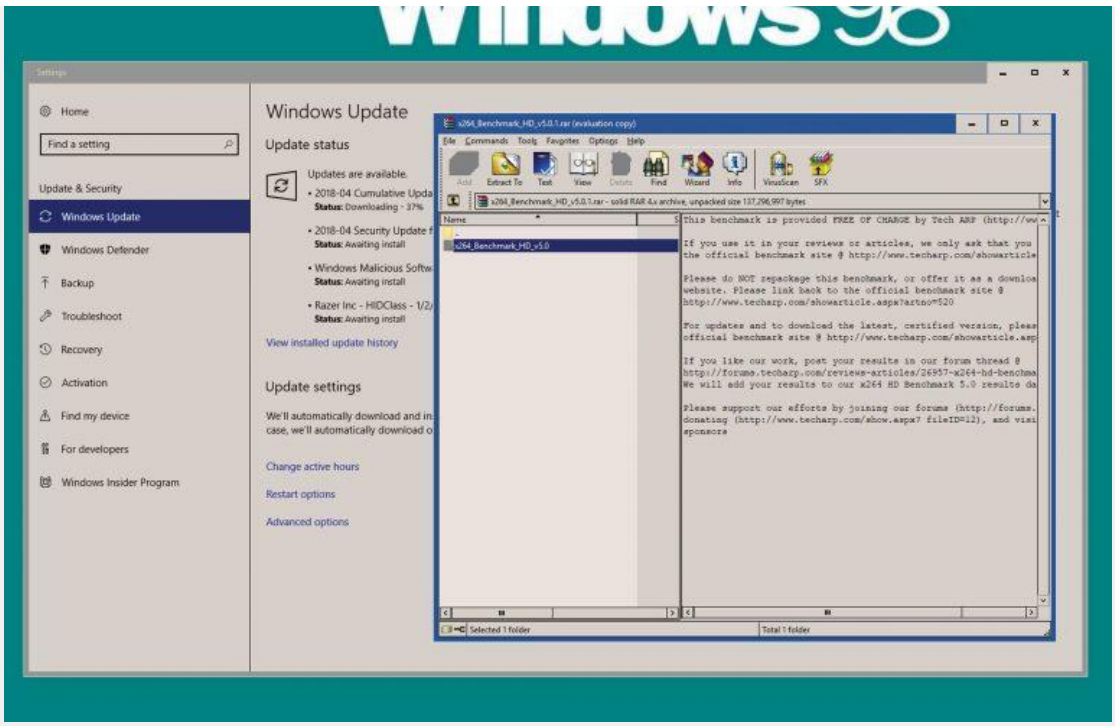
Helt åbenlyst er der naturligvis ingen grund til at køre cpu-benchmarks for at tjekke, om din ydelse er påvirket af patches, du måske aldrig har installeret. Så lad os tjekke, at du har. Sandsynligvis har dit OS, din browser og andre programmer allerede sørget for det, men bare for at være sikker: Gå til Windows Update ved at skrive "Windows Update" i søgefeltet og klik på programmet, når det dukker op. Under "Opdateringsstatus" klikker du på "Søg efter opdateringer" for at sikre, at du ikke har nogle ventende opdateringer. Hvis du har, så få dem installeret med det samme [Billede A]. Det er også værd at undersøge, om du har den seneste nye version af din webbrowser og installerer alle ventende programopdateringer. Det inkluderer antivirussoftware.



Billede A

2 Installer den påkrævede software

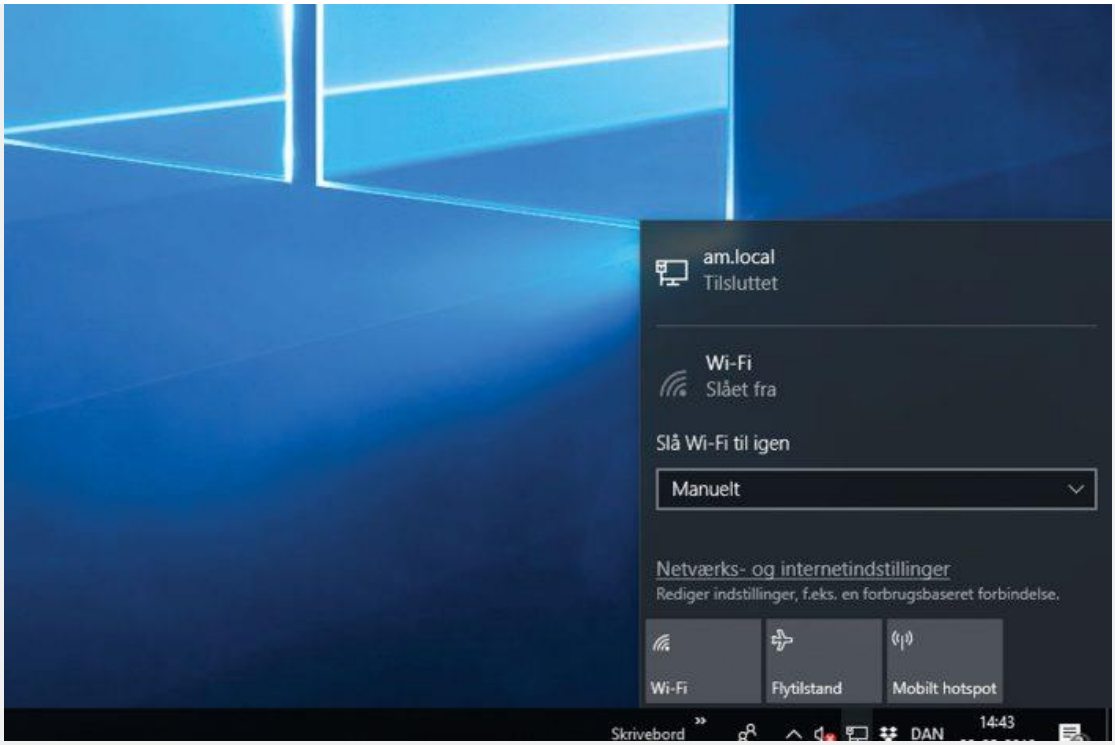
Du har brug for to programmer til at vurdere din før- og efter-ydelse korrekt i forhold til de sikkerheds-patches, du har installeret. Den første, InSpectre, fortæller dig, om dit system er beskyttet imod de to sårbarheder. Vi bruger x264 1080p encoding benchmark [Billede B] for at vurdere ydelsen, men du kan naturligvis bruge en hvilken som helst cpu-benchmark, du ønsker, så længe den i sidste ende giver dig et tal, du kan bruge til at sammenligne med andre kørsler. Hvis InSpectre fortæller dig, at dit system ikke er beskyttet, så gentag trin 1. Ellers er dit benchmark-værktøj installeret, og du er klar til at fortsætte.



Billede B

3 Undgå forstyrrelse ved at gå offline

Målet er at køre samme benchmark på det samme system under præcis de samme betingelser. Den eneste variabel bør være, om dine cpu sikkerheds-patches er aktiveret eller ej. For at gøre dette, så lad os undgå risikoen for, at en internetforbindelse eller aktivitet på hukommelsesdrevet kan forstyrre resultaterne. Du ved aldrig, hvornår GeForce Experience måske beslutter, at det er det perfekte tidspunkt til at installere nye grafikdrivere og sende din skærm ind i et midlertidigt mørke. Du bør gå midlertidigt offline uanset, om det betyder, at du skal trække et Ethernet-kabel eller USB trådløs modtager ud, eller bare deaktivere Wi-Fi nederst til højre i startbjælken [Billede C].

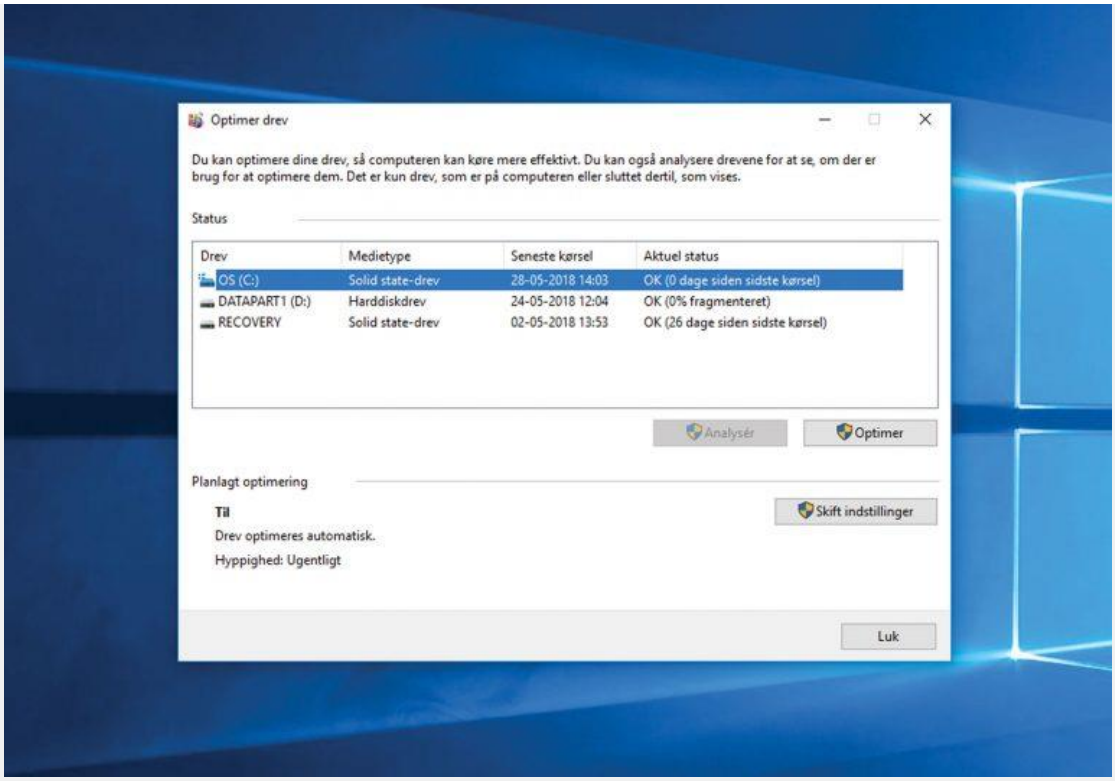


Billede C

4 Gør din lagerplads klar til test

Meltdown og Spectres fixes påvirker ikke kun din cpu-ydelse i vakuum. Din cpu er ansvarlig for softwaredefineret hukommelse (såsom partitioner), og størrelsen på den arbejdsbyrde, er de fleste enige om, påvirkes af sikkerheds-patches. Alt dette betyder, at hvis vores måling skal være præcis, så skal disk-aktiviteten være det samme under begge test-målinger. Det er derfor, vi går offline, og det er derfor, at vi anbefaler at køre en TRIM på din ssd, før du begynder på benchmarks.

Bare rolig, hvis din Windows er installeret på en HDD på din maskine, er tallene formodentlig så lave i første omgang, at ydelsesforskellene vil være ubetydelige. Ssd-brugere kan søge på “Optimer Drev” i søgefeltet i menubjælken [Billede D], og vælge det drev, du vil optimere. Dette starter TRIM – det er grundlæggende en defragmentering for solid-state-drev, der renser data-celler og rydder op steder, hvor der bliver skrevet data. Nu ved du, at din disk ikke installerer noget i baggrunden under benchmark-testen, som den lige har downloadet eller, som har hobet sig op ved, at du længe ikke har kørt TRIM-kommandoen.



Billede D

5 Benchmark og benchmark igen

Nu er tiden kommet til at samle noget data, du kan bruge til at analysere, om du har tabt ydelse. Du kan foretage den følgende procedure i en hvilken som helst rækkefølge, men for enkelthedens skyld, kører vi først benchmark-testen, mens Meltdown og Spectre -patchene er deaktiverede. Åben InSpectre for at gøre dette og klik på den ildevarslende “Disable Meltdown Protection”-knap i bunden af programmet. Efter endnu engang at have samlet dig mod til, så klikker du på “Disable Spectre Protection”-knappen ved siden af. Godt vi gik offline ikke? InSpectre burde fortælle dig med skræmmende røde bogstaver, at du ikke er beskyttet. Genstart dit system, sørg for at tjekke, at du stadig er offline, og vent på at alle startup-programmer kører.

Nu er det tid til benchmark. Vi tager tre 1080p encoding kørsler i x264 for at beregne et gennemsnit, bare for lidt mere præcision i sidste ende.

>> Med disse tre tal gemt, vil vi snuppe en bid brugbar data mere ved at udpakke x264 installerings-RAR-folderen på dit
skrivebord tre gange, og notere, hvor lang tid det tager hver gang. Dette giver os et indblik i disk-tilgangen samt rå cpu-kræfter i en syntetisk benchmark.

>> Det er endelig blevet tid til at varme os i Meltdown og Spectre-beskyttelsestæppet igen, så åben bare InSpectre og slå de to muligheder til igen i bunden af vinduet. En beroligende grøn skrift skulle nu gerne fortælle dig, at du atter er sikker igen. Pyha! Genstart din pc, genetabler din internetforbindelse og lad atter dine startprogrammer køre. Endelig kan du køre x264 eller dit udvalgte benchmark-software tre gange mere, og derefter udpakke installations-folderen på dit skrivebord tre gange mere og notere tiden.

6 Se forskellen – og græd stille

Forskellene på dine tal vil variere fra system til system. De vil formodentlig repræsentere 3-15 procents nedgang i ydelsen, når Meltdown og Spectre-beskyttelsen er aktiveret, med dine dekomprimersingstal, der ligger i den høje ende, mens cpu-ydelse vil variere marginalt mere. Hvis du ser ændringer mere end dette, er der næsten helt sikkert ugler i mosen, så skyd ikke bare skylden på patches. Kør nogle flere test og sørg for, at andre variabler ikke påvirker dine tal.

> Er 3–15 procent påvirkning af ydelsen acceptabel? Når man tager de skræmmende konsekvenser i betragtning, hvis nogen bruger Meltdown eller Spectre-sårbarhederne til at tilgå dine kodeord og andre personlige informationer, så ja.

Ingen ydelsestab vil blive budt velkommen med åbne arme, men heldigvis ser det ud til, at påvirkningen af fixene ikke er noget, de fleste vil bemærke i den daglige brug.

Kogepunktet

Hvordan opstod disse to berygtede cpu-problemer i første omgang? Og hvorfor tog det over 20 år for producenterne at opdage, at deres arkitektur repræsenterede en risiko? Svarene på disse presserende spørgsmål er endnu ikke kommet, og måske endnu mere skræmmende er det faktum, at de blev opdaget helt tilfældigt af tre forskellige og uafhængige forskningshold næsten samtidig.

At sårbarhederne påvirker cpu'er helt tilbage til 1995, men ikke var opdaget og forelagt Intel før juni 2017, antyder, at mange tidligere forskere var klar over det, men ikke handlede på det. Det er mere beroligende at forestille sig, at det var et rent tilfælde, så lad os holde fast i den teori. Før deres opdagelse var det længe anset som sandhed, at virtuel hukommelsesdata i cpu-cachen var så god som under lås og slå. Processer kunne simpelthen ikke tilgå data uden den rette bemyndigelse – troede alle fejlagtigt.

Både Meltdown og Spectre fungerer på næsten samme måde ved at tilgå cpu cache og al den rigdom, den indeholder. Og fordi problemet er grundlæggende i cpu-arkitektur, der har været gentaget over 25 år, er næsten enhver Intel- og AMD-processor, der er produceret i denne periode, påvirket.