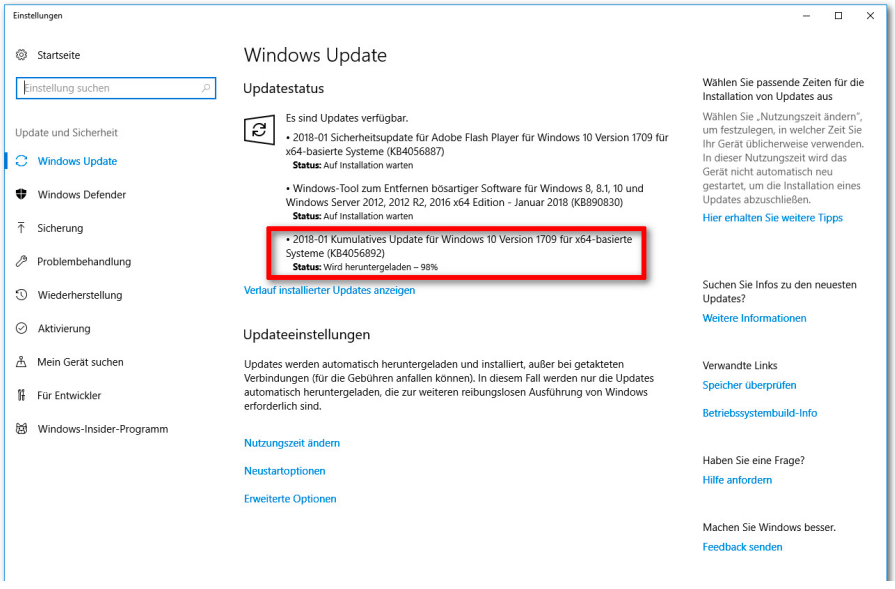
Benchmarks zu Meltdown und Spectre

SICHERHEIT STATT LEISTUNG?

Die ersten Windows- und BIOS-Updates gegen die Sicherheitslücken Meltdown und Spectre sind da. Wir testen mit Benchmarks, ob und wie stark die Performance in Spielen & Co darunter leidet. Von Nils Raettig

Seit Anfang des Jahres wissen wir, dass fast alle momentan relevanten Prozessoren von den Sicherheitslücken Meltdown und insbesondere Spectre betroffen sind. Wie groß das Risiko genau ist, lässt sich nach wie vor schwer einschätzen, inzwischen gibt es aber immerhin die ersten Windows- und BIOS/UEFI-Updates. Wir haben passende Benchmarks durchgeführt, die die Gaming-Performance und die Anwendungsleistung von Prozessoren vor und nach der Installation der Patches miteinander vergleichen.

Dabei beschränken wir uns aus zwei Gründen zunächst auf Modelle von Intel: Einerseits sind AMD-CPUs inklusive der aktuellen Ryzen-Prozessoren wie etwa dem Ryzen 5 1600 laut offiziellen Angaben nicht von Meltdown betroffen, die Gegenmaßnahmen im entsprechenden Windows Update greifen hier also nicht. Andererseits gab es zum Testzeitpunkt für die von uns verwendeten AMD-Mainboards noch keine passenden Microcode-Updates, die sich Spectre widmen würden. Erste Gegentests auf AMD-Systemen mit den neuesten Windows-Updates zeigten erwartungsgemäß keine Leistungsunterschiede. Hier lohnt es sich also erst nach der Veröffentlichung von Microcode-Updates, genauer hinzusehen.



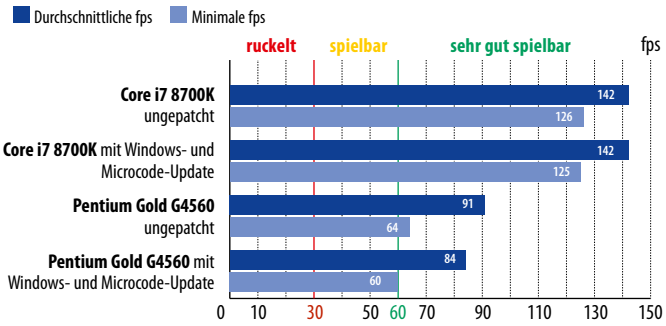
Unter Windows 10 bringt das Update KB4056892 Gegenmaßnahmen zu Meltdown mit sich. Auch für Windows 8.1 und Windows 7 sind entsprechende Updates erschienen.

Wo bekomme ich die Updates her?

Bevor wir uns den Benchmarks widmen, klären wir zunächst, von welchen Sicherheits-Updates wir hier genau reden. Gegen Meltdown, das primär Intel-CPUs und einige wenige ARM-Prozessoren betrifft, hat Microsoft Updates für Windows 10 (KB4056892), Windows 8.1 (KB4056898) und Windows 7 (KB4056897) veröffentlicht, die seit dem 09.01.2018 regulär über die Update-Funktion verteilt werden. Auf all unseren Testsystemen läuft inzwischen Windows 10, der passende Patch wurde hier stets über die Windows-Update-Funktion ohne weiteres Zutun von uns installiert. Gleiches sollte auch für ältere Windows-Versionen gelten. Über den offiziellen Update-

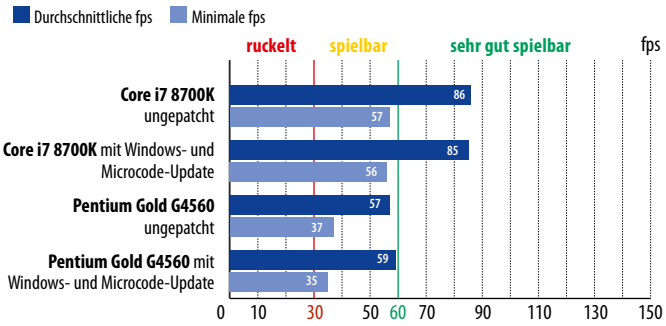
Spiele-Benchmarks

Battlefield 1 — Full HD, hohe Details, TAA, DX11



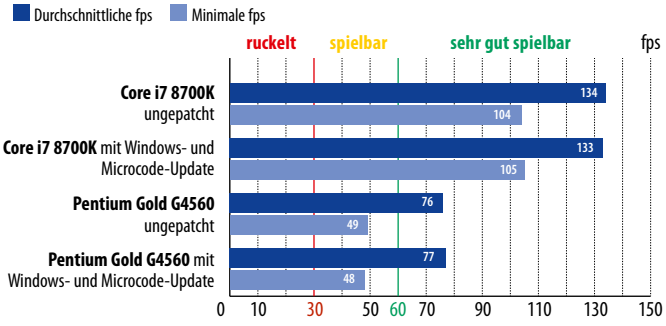
Gemessen in fps. Je höhher, desto schneller.
Unter 30 fps nicht mehr gut spielbar.

Rise of the Tomb Raider (DX 11) — Full HD, hohe Details, SMAA



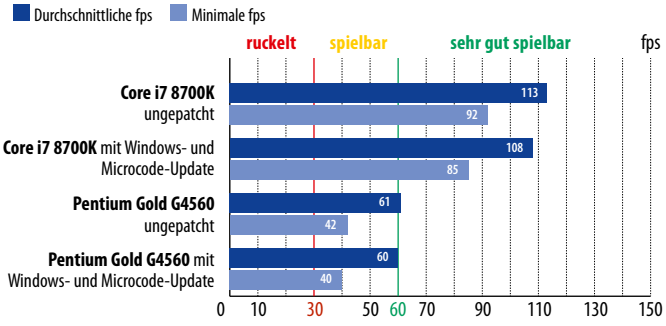
Gemessen in fps. Je höhher, desto schneller.
Unter 30 fps nicht mehr gut spielbar.

The Witcher 3 — Full HD, hohe Details, Hairworks deaktiviert



Gemessen in fps. Je höhher, desto schneller.
Unter 30 fps nicht mehr gut spielbar.

Rise of the Tomb Raider (DX 12) — Full HD, hohe Details, SMAA



Gemessen in fps. Je höhher, desto schneller.
Unter 30 fps nicht mehr gut spielbar.

Katalog auf der Internetseite www.catalog.update.microsoft.com und die Suche nach der Update-Bezeichnung ist aber auch der manuelle Download möglich.

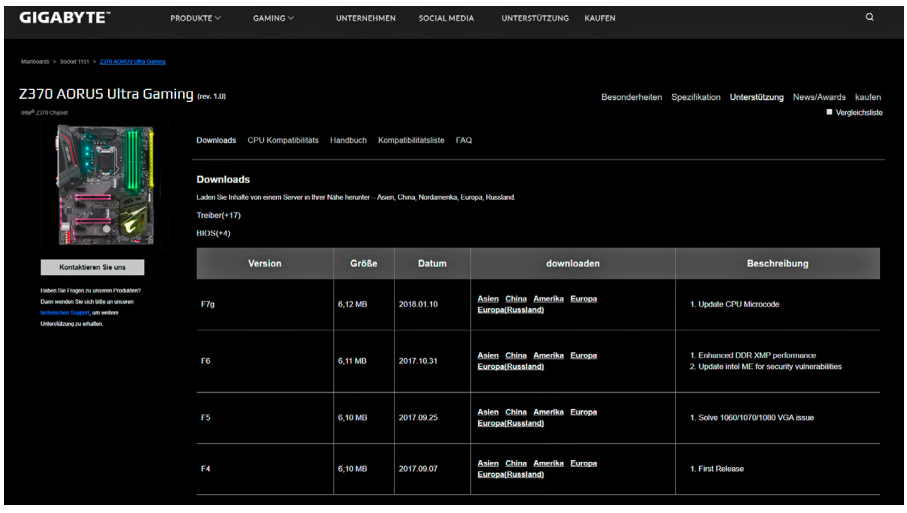
Vorsicht auf Rechnern mit AMD-Prozessoren: Hier kann es in Einzelfällen durch die Installation der Updates zu Boot-Problemen und anderen Schwierigkeiten kommen. Betroffenen soll das nachgereichte Update KB4073290 helfen, das nur für AMD-PCs bereitgestellt wird. Auf unseren Test-Rechnern sind keine Schwierigkeiten dieser Art aufgetreten. Wir raten aber dennoch dazu, wichtige Daten zu sichern, falls die Updates auf eurem PC nicht ohnehin schon installiert wurden. Um zu überprüfen, ob das der Fall ist, hilft ein Blick in den Installations-Verlauf. Klickt dazu in den Windows-Einstellungen auf »Update und Sicherheit« und dann im rechten Fensterbereich auf »Verlauf installierter Updates anzeigen«. Hinter den einzelnen Einträgen steht jeweils in Klammern die Nummer des Updates, im Falle von Windows 10 müsst ihr hier also beispielsweise nach »KB4056892« Ausschau halten.

Bei Spectre gestaltet sich die Situation etwas unübersichtlicher, auch da die Sicherheitslücke in unterschiedlichen Varianten auftreten kann. Neben Software-Updates für das Betriebssystem und für Anwendungen wie vor allem Internet-Browser sind als Gegenmaßnahme auch Microcode-Updates für die Hardware notwendig.

Neuer Microcode ist Pflicht

Im Falle von Desktop-PCs mit aktuellen Intel-CPUs der Generationen Coffee Lake (Core i 8000), Kaby Lake (Core i 7000) und Skylake (Core i 6000) gibt es inzwischen für viele Mainboards auf den Support-Seiten entsprechende BIOS- beziehungsweise UEFI-Updates, die sich mit den Anleitungen der Hersteller und passenden Tools meist leicht installieren lassen. Wir haben dazu immer den Weg über einen USB-Stick gewählt, auf dem die entsprechende Update-Datei gespeichert werden muss. Anschließend öffnet man beim Booten des PCs das UEFI (in der Regel per Druck auf die »Entfernen«-Taste), startet dort das Update-Tool (beim Finden hilft oft ein Blick in das Mainboard-Handbuch oder eine schnelle Websuche) und wählt die Datei auf dem Stick aus. Der Update-Vorgang an sich dauert unserer Erfahrung nach meist weniger als eine Minute.

Auf manchen PCs kann es in Folge des BIOS-Updates passieren, dass der Rechner ab und zu ungewollt neu startet. Das hat Intel auch offiziell bestätigt, man arbeitet bereits an einer Lösung und stellt neue Microcode-



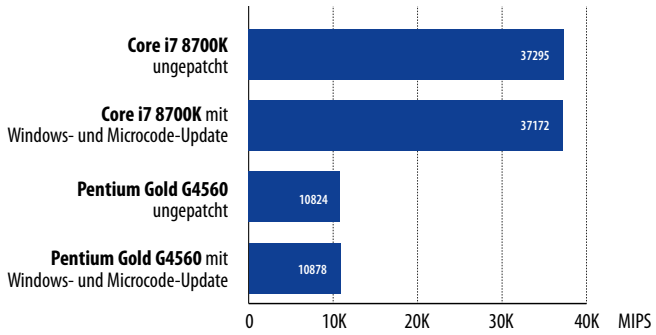
Für aktuelle Intel-Prozessoren bieten mittlerweile viele Mainboard-Hersteller UEFI-Updates zum besseren Schutz an. Meist steht in der Beschreibung »Microcode-Update« oder ähnliches.

Bei Geräten wie Notebooks seid ihr darauf angewiesen, dass der jeweilige Hersteller ein passendes Microcode-Update bereitstellt.

Anwendungs-Benchmarks

7-Zip integrierter Benchmark

Angabe in Millionen Instruktionen pro Sekunde. Je mehr, desto besser.



Updates in Aussicht. Für eine höhere Sicherheit rät Intel aber dazu, dennoch die neuesten BIOS-Versionen mit Spectre-Gegenmaßnahmen zu installieren und sie nicht etwa wieder zu deinstallieren. Microsoft hat außerdem inzwischen das Windows-Update KB40788130 bereitgestellt, dass die Microcode-Updates softwareseitig wieder deaktiviert. Installieren sollten das Update aber nur Nutzer, bei denen tatsächlich Abstürze und Neustarts wegen des neuen Intel-Microcodes auftreten. Bei unseren Rechnern war das übrigens nie der Fall. Letztlich muss aber jeder selbst entscheiden, ob er noch eine Zeit auf angepasste Microcode-Updates wartet oder lieber jetzt schon die ersten Versionen davon installiert.

Auf welchem Weg ihr herausfindet, ob ihr alle verfügbaren Windows-Updates und Microcode-Aktualisierungen gegen Meltdown und Spectre erfolgreich für einen besseren Schutz installiert habt, zeigt euch der Kasten » Sicherheitscheck mit der Powershell« auf der letzten Seite dieses Artikels.

Ältere Hardware, Notebooks & Co

Schwieriger sieht es in Sachen Microcode-Updates mit älteren CPU-Generationen wie Haswell (Core i 4000), Ivy Bridge (Core i 3000) oder Sandy Bridge (Core i 2000) aus. Zum Testzeitpunkt gab es noch keine entsprechenden Microcode-Updates, gleiches gilt für AMD-Plattformen. Das dürfte sich aber im Laufe der Zeit ändern, hier lohnt sich also ein regelmäßiger Blick auf die Support-Seite des Mainboard-Herstellers. Besitzt ihr dagegen einen Komplett-PC, ein Notebook oder ein anderes Gerät, das nicht auf eine einzeln im Handel erhältliche Hauptplatine setzt, seid ihr darauf angewiesen, ein entsprechendes Microcode-Update vom System-Hersteller zu bekommen.

Das könnte in Einzelfällen allerdings noch eine ganze Weile dauern, da vor allem etwas ältere Systeme unserer Erfahrung nach häufig nicht mit regelmäßigen Updates versorgt werden. Für diese Fälle empfehlen wir euch, direkten Kontakt mit dem Anbieter eures PCs aufzunehmen. Einerseits besteht die Möglichkeit, dass es bereits ein Update gibt, das aber nicht so leicht auf den offiziellen Support-Seiten zu finden ist. Andererseits dürften solche Anfragen die Wahrscheinlichkeit erhöhen, dass überhaupt an einem passenden Update gearbeitet wird.

Benchmarks unter Windows 10

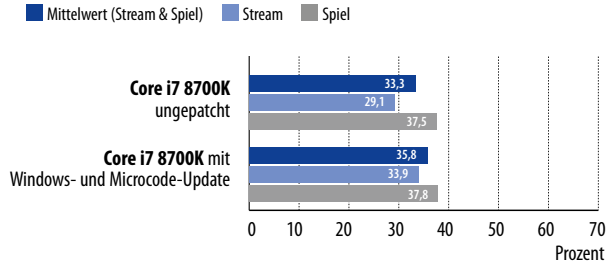
Wir haben uns für Messungen mit zwei verschiedenen Prozessoren von Intel unter Windows 10 entschieden. Einerseits für den Core i7 8700K (Coffee-Lake-Generation) mit sechs Kernen, der im Mainstream-Bereich die aktuell schnellste CPU von Intel darstellt. Andererseits für den Pentium Gold G4560 (Kaby-Lake-Generation), der als Einsteiger-CPU sehr beliebt ist, aber nur über zwei Kerne verfügt. Im Falle des Core i7 8700K nutzen wir das Gigabyte Z370 Aorus Ultra Gaming in der BIOS-Version F7g, beim Pentium kommt das Asus ROG Maximus IX Hero in der Version 1203 zum Einsatz. Wir vergleichen dabei die Benchmark-Ergebnisse aus unserem CPU-Testsystem ohne Windows- und BIOS-Update für Meltdown und Spectre mit den Messungen nach der Installation dieser Updates.

Außerdem haben wir neue Messungen zu der Geschwindigkeit einer SSD durchgeführt (Samsung SSD 830 Evo), da es Berichte über deutliche Performance-Einbußen bei Laufwerken mit Flash-Speicher gibt. Dass wir die Auswirkungen des Windows- und BIOS-Updates gemeinsam testen statt jeweils auch Messungen mit nur einem der beiden Updates durchzuführen, hat vor allem zwei Gründe: erstens der größere Zeitaufwand, zweitens die Tatsache, dass es klar empfehlenswert ist, beide Aktualisierungen statt nur eine davon zu installieren. Für die Zukunft sind weitere Testszenarien denkbar:

Streaming-Benchmarks

Battlefield 1

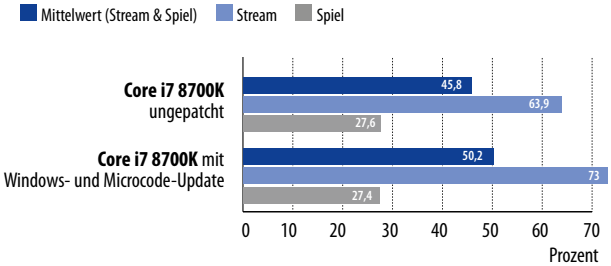
verlorene Frames in Prozent, Stream per OBS zu Twitch.tv
(1080p, Preset Medium, Bitrate 5.000, 60 fps, x264)



Angaben in Prozent. Je niedriger, desto besser.

The Witcher 3

verlorene Frames in Prozent, Stream per OBS zu Twitch.tv
(1080p, Preset Medium, Bitrate 5.000, 60 fps, x264)

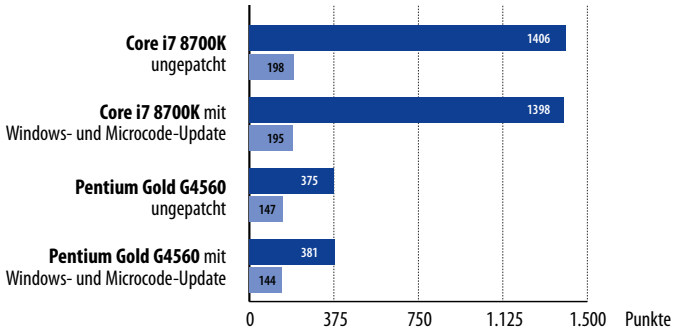


Angaben in Prozent. Je niedriger, desto besser.

Testsystem: Nvidia Geforce GTX 1080, 16,0 GByte Arbeitsspeicher, Windows 10

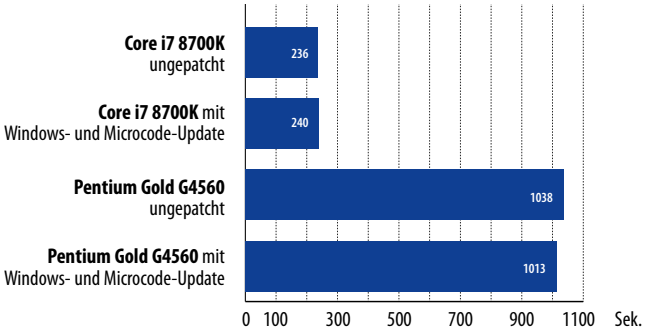
Cinebench R15 CPU-Test

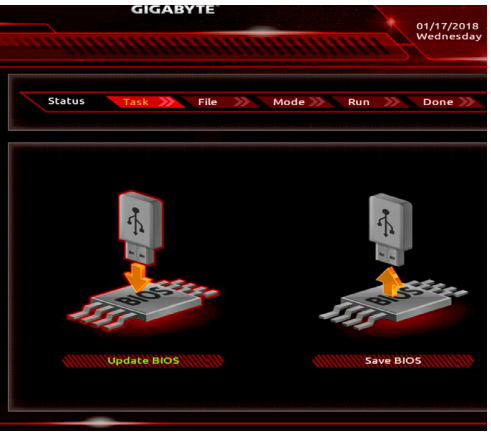
Angabe in Punkten. Je mehr, desto besser. Multicore Singlecore



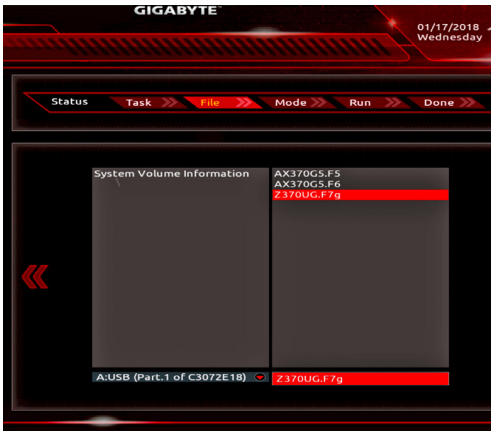
Handbrake Encodierung eines 4K-Videos (H.265)

Angabe in Sekunden. Je weniger, desto besser.

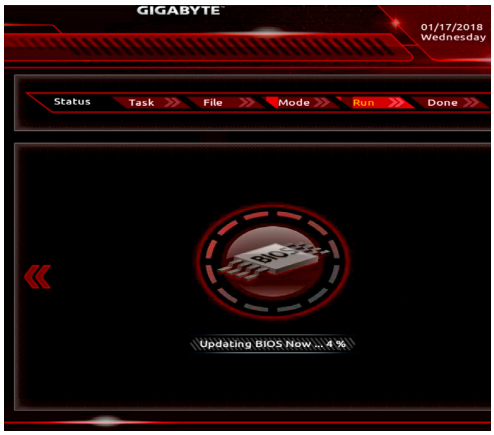




Um die Microcode-Updates für höhere Sicherheit zu installieren, haben wir Update-Tools im BIOS genutzt, hier am Beispiel des Gigabyte 370 Aorus Ultra Gaming zu sehen.



Das Tool nennt sich in diesem Fall Q-Flash. Die Update-Datei haben wir nach dem Download auf der Support-Seite des Mainboards auf einen USB-Stick kopiert, um sie beim Installationsvorgang auswählen zu können.



Der Update-Vorgang selbst ist meist in weniger als einer Minute erledigt. Es kann allerdings sein, dass der PC danach zwei, drei Mal neu starten muss, bis alle Änderungen umgesetzt sind.

Mit AMD-Prozessoren, wenn die entsprechenden Microcode-Updates da sind. Mit älteren Intel-CPUs wie dem Core i7 2600K, die schon jetzt von dem Windows-Update für Meltdown betroffen sein können, für die aber ebenfalls noch Microcode-Updates ausstehen. Außerdem dürfte sich ein Blick auf das immer noch bei vielen sehr beliebte Windows 7 lohnen, für das Microsoft selbst von höheren Performance-Einbußen als unter Windows 10 ausgeht.

Aufgrund der großen Zahl von verschiedenen Prozessoren, Hardware-Kombinationen und Anwendungen sowie mehrerer Windows-Versionen ist es mit solchen Tests aber generell nur möglich, einen sehr begrenzten Ausblick auf die Leistungsauswirkungen der Sicherheitsupdates in ausgewählten Szenarien zu geben. Oder anders ausgedrückt: Bestimmte Programme, Spiele und PCs können deutlich stärker oder auch viel weniger stark davon betroffen sein, als es in unserem Test der Fall ist.

Gaming- und Streaming Benchmarks

Mit Blick auf die Spiele-Benchmarks zeigt sich der Core i7 8700K in den von uns getesteten Titeln größtenteils unbeeindruckt von den Sicherheits-Updates. Die Unterschiede schwanken meist im Rahmen der Messgenauigkeit, mit einer Ausnahme: Unter DirectX 12 sinken die durchschnittlichen fps in Rise of the Tomb Raider immerhin um fünf Prozent, die minimalen fps um acht Prozent. Unter DirectX 11 sind im gleichen Spiel keine ähnlichen Unterschiede zu beobachten, was durchaus in das Bild passt. DirectX 12 soll schließlich unter anderem für eine bessere Ausnutzung der Prozessorleistung sorgen und kann die fps in Rise of the Tomb Raider oft deutlich erhöhen – dementsprechend klingt es plausibel, dass die Sicherheits-Patches hier eher negative Auswirkungen haben. Beim Pentium Gold G4560 gibt es diesen Unterschied zwischen DX11 und DX12 in Tomb Raider nicht, allerdings profitiert dieser Prozessor im Gegensatz zum Core i7 8700K ohnehin kaum vom Wechsel der Schnittstelle. Dafür messen wir in Battlefield 1 einen Performance-Verlust von etwa sieben bis acht Prozent, während die Leistung im Rollenspiel The Witcher 3 weitgehend identisch bleibt.

Ein interessantes Ergebnis zeigt sich bei den Streaming-Benchmarks. Wir beschränken uns hier auf den Core i7 8700K und das vergleichsweise fordernde Streaming in 1080p mit 60 Bildern pro Sekunde und dem Preset »Medium«. Während die fps im Spiel selbst nicht stärker sinken als ohne die Sicherheits-Updates, sieht es bei der Darstellung des Streams anders aus. In Battlefield 1 gehen 34 Prozent statt zuvor 29 Prozent der Bilder des Streams verloren. In The Witcher 3 sind es sogar 73 Prozent statt zuvor knapp 64 Prozent. Da bei einem Stream möglichst überhaupt keine Bilder verloren gehen sollten, macht das in diesen Fällen zwar keinen entscheidenden Unterschied – ruckelig war der Stream in beiden Spielen bereits ohne die Sicherheits-Updates. Das könnte aber anders aussehen, wenn ein Stream näher an der Null-Prozent-Marke bei den verlorenen Bildern liegt.

Anwendungen und SSDs

In den Anwendungs-Benchmarks unseres regulären CPU-Testsystems messen wir weder beim Core i7 8700K noch beim deutlich langsameren Pentium Gold G4560 nennenswerte Unterschiede durch die Meltdown- und Spectre-Sicherheits-Updates. Das lässt allerdings nicht automatisch Rückschlüsse auf andere Anwendungen zu. Bei den Daten-

raten mit einer älteren Samsung SSD 830 (SATA3) stellen wir dagegen größere Differenzen fest (aus Platzgründen sind die Benchmarks online unter bit.ly/2FS80l2 zu finden). Beim Lesen gibt es im AS-SSD-Benchmark zwar kaum Unterschiede, beim Schreiben sinken die Werte aber im 4KByte-Test mit vielen kleinen Datenblöcken immerhin um fast 15 Prozent.

Etwas anders verhält es sich mit Crystal Disk Mark. Während die Sicherheits-Updates in diesem Tool beim Lesen ebenfalls kaum einen Unterschied machen, fällt die Leistung beim Schreiben hier im sequentiellen Test mit größeren Datenblöcken und einem Thread deutlich ab. Die Kollegen von ComputerBase haben dagegen in ihren Benchmarks mit einer deutlich schnelleren Samsung SSD 960 Pro (M.2-Anbindung) an anderer Stelle Leistungseinbrüche festgestellt: Hier leidet vor allem die Performance beim 4KByte-Test mit kleinen Datenblöcken und einem Thread sowohl beim Lesen als auch beim Schreiben.

Die Sicherheits-Updates können also negative Auswirkungen auf die Leistung einer SSD haben. In welchem Bereich genau, scheint aber vom spezifischen Datenträger und möglicherweise auch vom jeweiligen System abzuhängen. Ebenfalls nicht zu vergessen: Performance-Verluste in synthetischen Benchmarks machen sich häufig nur sehr bedingt im PC-Alltag bemerkbar. Wir haben bei unseren Arbeiten an diesem Artikel zumindest keine längeren Ladezeiten in Spielen oder eine langsamere System-Performance auf den aktualisierten PCs festgestellt. Insgesamt machen sich die Sicherheits-Updates damit unseren bisherigen Eindrücken nach zu urteilen nicht spürbar negativ in Sachen Leistung bemerkbar. ★

Nils Raettig
@nraettig

Zugegeben, unsere ersten Benchmarks zu den Performance-Auswirkungen der Sicherheits-Updates gegen Meltdown und Spectre können nur einen begrenzten Ausblick geben. Die Situation wird außerdem zusätzlich durch die oft noch fehlenden Microcode-Updates für ältere Intel-Prozessoren und AMD-Systeme erschwert. Dass es in Einzelfällen durchaus spürbare Leistungsabfälle geben kann, ist aber wohl gewiss. Für Spieler lautet die gute Nachricht meinen bisherigen Eindrücken nach zu urteilen, dass sich die Performance-Unterschiede in Spielen maximal im einstelligen Prozentbereich bewegen und dass es häufig gar keine messbaren Differenzen gibt. Ich bin sehr gespannt darauf, wie sich die Situation bei älteren Prozessoren wie dem Core i7 2600K und Betriebssystemen wie Windows 7 darstellen wird.

AMD-Prozessoren wie die Threadripper-Modelle oder die kleineren Ryzen-CPUs sind nach aktuellen Stand nur von der Sicherheitslücke Spectre und nicht von Meltdown betroffen.

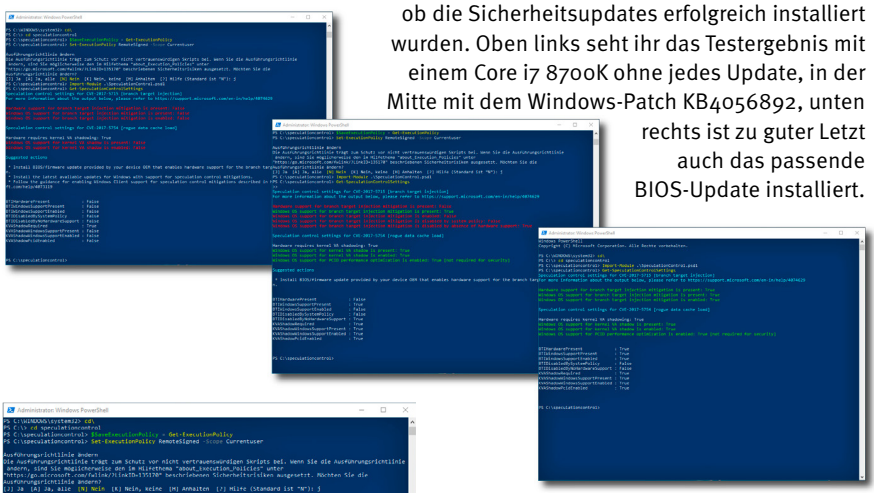
Sicherheitscheck mit der Powershell

Um sicherzugehen, dass die Updates gegen Meltdown und Spectre erfolgreich installiert wurden, hilft ein von Microsoft zur Verfügung gestelltes Script (zu finden auf der Webseite aka.ms/SpeculationControlPS) für die Eingabeaufforderung per Powershell. Auf unseren Rechnern hat unter Windows 10 stets das folgende Vorgehen eine zuverlässige Ausführung des Scripts ermöglicht.

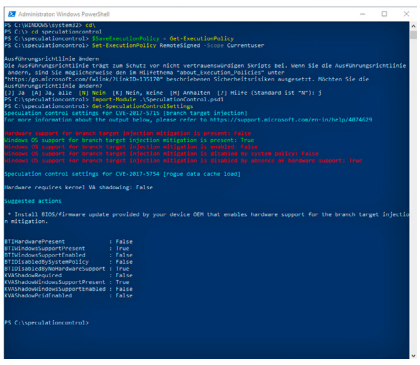
- Entpacken der Zip-Datei (etwa in den Ordner »C:\SpeculationControl)
- »PowerShell« im Suchfeld des Startmenüs eingeben, rechts auf den entsprechenden Eintrag klicken und »Als Administrator ausführen« auswählen
- Die folgenden Befehle eingeben:
- **$SaveExecutionPolicy = Get-ExecutionPolicy**
- **Set-ExecutionPolicy RemoteSigned -Scope Currentuser**
- Sicherheitsabfrage mit »**J**« und der Enter-Taste bestätigen und weitere Befehle eingeben:
- **cd c:\SpeculationControl**
- **Import-Module .\SpeculationControl.psd1**
- **Get-SpeculationControlSettings**

Danach sollte man laut Microsoft noch den Befehl **Set-ExecutionPolicy $SaveExecutionPolicy -Scope Currentuser** eingeben und die Anfrage wieder mit »J« und Enter bestätigen, um die Ausführungsrichtlinien zurückzusetzen. Die erste Gruppe von Einträgen mit »True«- oder »False«-Angaben (»branch target injection«), die über das Script ausgegeben wird, widmet sich Spectre in der Variante 2, die nächste Meltdown (»rogue data cache load«). Grüne Einträge stehen für verbesserten Schutz, rote für fehlenden.

Auf unseren Intel-PCs waren alle Einträge grün markiert, nachdem wir das Windows-Update und das Microcode-Update installiert haben. Bitte beachtet allerdings, dass das nicht mit einem völligen Schutz gleichzusetzen ist, da für Spectre in der Variante 1 anwendungsspezifische Updates nötig sind. Wer nicht auf die PowerShell zurückgreifen möchte, der kann auch Tools wie den »Spectre Meltdown CPU-Checker« von Ashampoo (bit.ly/2nrHnrb) oder »inSpectre« von Steve Gibson (bit.ly/2DEQkXw) nutzen, um zu prüfen, ob die Schutzmaßnahmen aktiv sind. Letzteres bietet sogar die Möglichkeit, die Maßnahmen wieder zu deaktivieren (auch wenn das höchstens beim Auftreten von PC-Problemen zu Testzwecken sinnvoll ist).



Mit einem PowerShell-Script könnt ihr überprüfen, ob die Sicherheitsupdates erfolgreich installiert wurden. Oben links seht ihr das Testergebnis mit einem Core i7 8700K ohne jedes Update, in der Mitte mit dem Windows-Patch KB4056892, unten rechts ist zu guter Letzt auch das passende BIOS-Update installiert.



Mit AMD-Prozessoren (in diesem Fall dem Ryzen 7 1800X) sieht das Testergebnis des PowerShell-Scripts etwas anders aus, da diese CPUs nicht von Meltdown betroffen sind. Microcode-Updates gab es zum Testzeitpunkt für AMD-Modelle aber noch nicht, daher können wir diese auch vom Powershell-Skript empfohlene Maßnahme für (partiellen) Schutz vor Spectre (noch) nicht ergreifen.