Raytracing kommt für Computerspiele

Die Star-Wars-Raytracingdemo Unreal Engine 4 sieht nahezu fotorealistisch aus, benötigt aber die Rechenleistung von vier Volta-Grafikkarten.

Microsoft erweitert DirectX 12 um die neue Schnittstelle DirectX Raytracing (DXR). Sie ermöglicht es Spieleentwicklern, bestimmte 3D-Effekte durch Raytracing statt Rasterizing zu berechnen. Damit lassen sich fotorealistische 3D-Szenen erstellen – allerdings benötigt Raytracing wesentlich mehr Rechenleistung als das etablierte Rasterizing-Verfahren.

Zeitgleich hat Nvidia das Raytracing-Backend RTX angekündigt, das über Microsofts DXR auf die GPU zugreift. Nvidia RTX richtet sich zunächst an Spieleentwickler, die über die Gameworks-Entwicklungsumgebung Raytracing-Implementierungen für Area Shadows, Glossy Reflections und Umgebungsverdeckung (Ambient Occlusion) umsetzen können. Raytracing Area Shadows und Glossy Reflections soll ab März verfügbar sein, Raytraced Ambient Occlusion folgt im Sommer 2018.

Nvidia zufolge werden DXR und Nvidia RTX von den 3D-Engines Unity, Frostbite, Unreal Engine und Allegorithmic unterstützt; außerdem sollen die Spielefirmen EA, Remedy und 4A Games im Boot sein. Erste Spiele mit Raytracing-Effekten sollen noch in diesem Jahr erscheinen.

Nvidia RTX läuft allerdings nur mit Volta-Grafikchips und deren Nachfolgern – die einzige Volta-Grafikkarte mit Display-Anschluss ist die 3100 Euro teure Nvidia Titan V. Die eigentlich für K.I.-Berechnungen gedachten Tensor Cores, die nur in Volta-GPUs stecken, können über Denoise-Berechnungen die allgemeine Raytracing-Performance weiter beschleunigen.

AMD hat bislang kein Backend für DXR angekündigt, aber auf einen zukünftigen Raytracing-Treiber verwiesen. Über einen Fallback-Compute-Layer lässt sich Microsofts DXR auch ohne Spezialtreiber mit bisherigen GPUs von AMD und Nvidia nutzen. Dieser Weg dürfte allerdings nicht so leistungsfähig wie angepasste Raytracing-Treiber sein.

Das Raytracing-Verfahren folgt der natürlichen Ausbreitung des Lichts nach den Gesetzen der Strahlenoptik – allerdings in umgekehrter Richtung: Ausgehend vom Auge eines virtuellen Beobachters schickt es für jeden Bildpunkt einen „Sehstrahl“ in die darzustellende Szene. Das Objekt, auf den der Punkt zuerst trifft, ist dann sichtbar. *(mfi@ct.de)*

Sicherheitslücken in AMD-Prozessoren

Die israelische Firma CTS-Labs hat in Ryzen- und Eypc-Prozessoren sowie den AMD-Chipsätzen für die Plattformen AM4 (Ryzen) und TR4 (Ryzen Threadripper) insgesamt zwölf Sicherheitslücken gefunden. Die in den vier Gruppen Chimera, Fallout, Masterkey und Ryzenfall eingeteilten Lücken lauern unter anderem im Platform Security Processor (PSP), der seit 2014 in AMD-Prozessoren steckt, sowie in der Firmware der von der taiwanischen Firma Asmedia entwickelten Chipsätze.

Damit Angreifer die Sicherheitslücken ausnutzen können, müssen sie auf den Rechnern über Administrator-Rechte verfügen. Erst dann können sie mit viel Aufwand Schutzfunktionen wie das in der CPU verankerte Firmware-TPM (fTPM) sowie Secure Encrypted Virtualization umgehen. Zudem lässt sich laut CTS-Labs damit schwer zu entdeckende Malware im PSP, der UEFI-Firmware und im Chipsatz verankern.

AMD arbeitet zusammen mit Asmedia an Patches und will diese in den nächsten Wochen an PC- und Mainboard-Hersteller verteilen, damit diese sie in BIOS-Updates einbauen können. Mehrere Sicherheitsexperten übten Kritik am Vorgehen von CTS-Labs, weil die Firma die Lücken weniger als 24 Stunden, nachdem sie AMD kontaktiert hatte, veröffentlicht hat. Üblich ist eine Frist von 90 Tagen. *(chh@ct.de)*

Microcode-Updates für Spectre

Der Prozessorhersteller Intel hat weitere Microcode-Updates für die Spectre-V2-Sicherheitslücke veröffentlicht. Die Microcode-Updates rüsten drei Funktionen für Indirect Branch Control (IBC) nach, die zusammen mit Betriebssystem-Updates die Lücke Branch Target Injection (BTI, CVE-2017-5715) schließen. Der Linux Processor Microcode Data File enthält nun die IBC-Patches für alle Core-i-Prozessoren ab der zweiten Generation (Core i-2000), die seit 2011 erhältlich sind oder waren. Linux-Systeme mit diesen CPUs benötigen somit keine BIOS-Updates mit aktualisierten Microcodes.

Windows-10-Nutzer können das optionale Windows-Update KB4090007 installieren, welches Microcode-Updates mit IBC für Prozessoren der Serien Core i-6000 „Skylake“, i-7000 „Kaby Lake“ und i-8000 „Coffee Lake“ sowie deren Xeon-Äquivalente lädt.

Für Ende 2018 verspricht Intel erste Prozessoren, die Architekturänderungen gegen die Angriffszenarien Spectre 2 und Meltdown enthalten. Dafür hat der Chiphersteller nach eigener Aussage Teile der CPU umgestaltet, um zusätzliche „Schutzwände“ zwischen laufenden Anwendungen sowie Prozessen mit unterschiedlichen Zugriffsrechten zu errichten. Die ersten Prozessoren mit Hardwareschutz sollen die Serverchips Xeon-SP „Cascal Lake“ sowie nicht näher spezifizierte Core-i-Prozessoren der achten Generation sein. *(chh@ct.de)*

Microcode-Updates für Linux und Windows 10: **ct.de/ypc9**