Intel Xeon-AP soll mit 48 Kernen kommen

Für 2019 kündigt Intel eine besondere Variante von Serverprozessoren an: den **Xeon Advanced Performance** (Xeon-AP) mit 48 Kernen. Dabei geht es um Chips der neuen Generation Cascade Lake, die unter der Bezeichnung Cascade Lake-SP auch bald als Xeon Scalable Processors kommen sollen. Diese „Xeon-SP"-Prozessoren haben aber wie ihre aktuellen Vorgänger (Skylake-SP) höchstens 28 Kerne und passen auch auf dieselben LGA3647-Mainboards.

Anders der Cascade Lake-AP (CLX-AP), denn die 48-Kerner sind Multi-Chip-Packages (MCP) mit 12 statt bisher sechs DDR4-Speicherkanälen. Sie brauchen neue Fassungen, möglicherweise werden sie nur aufgelötet auf Mainboards zu haben sein. Intel verrät dazu noch keine Details, man munkelt von BGA5903-Gehäusen.

Zwei Xeon-AP lassen sich zusammenschalten für einen Dual-Socket-Server mit 96 Kernen und 24 RAM-Kanälen. Zum maximalen Speicherausbau, zur Zahl der PCI-Express-Lanes und zu Preisen verrät Intel bisher nichts. Manches spricht dafür, dass Intel schlichtweg zwei 24-kernige Cascade-Lake-SP-Chips in einem Gehäuse zusammenfasst: Ein Zwei-CPU-Server damit wäre quasi ein auf zwei physische Prozessoren eingedampftes Viersockelsystem.

Der Xeon-AP mit 48 Kernen ist dem aktuellen AMD Epyc 7601 mit 32 Kernen überlegen. 2019 will AMD allerdings die nächste Epyc-Generation „Rome" mit Zen-2-Technik bringen, die vermutlich bis zu 64 Kerne haben wird. *(ciw@ct.de)*

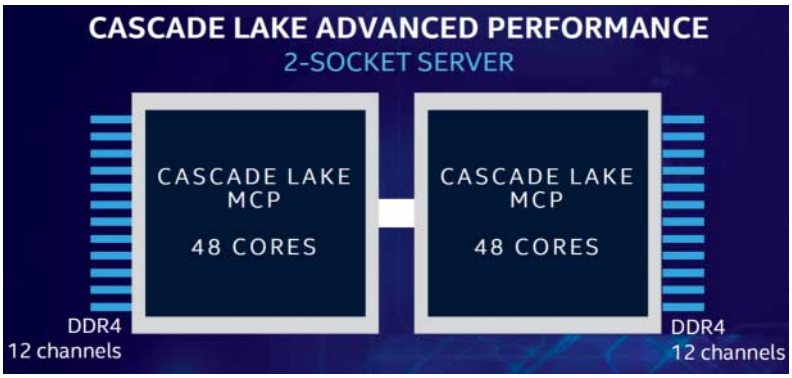

Bild: Intel

Intel kündigt den Serverprozessor Cascade Lake Advanced Performance mit 48 Kernen an.

PortSmash: Sicherheitslücke bei Hyper-Threading

Fünf Forscher von den Universitäten in Tampere (Finnland) und in Havanna (Kuba) haben die Sicherheitslücke PortSmash veröffentlicht. Dabei kann ein Thread, der auf einem logischen Kern eines Prozessors mit Hyper-Threading läuft, **Daten lesen, die der andere logische Kern gerade verarbeitet**. Die Forscher zeigten, dass sich damit ein geheimer, privater Schlüssel aus OpenSSL unter Ubuntu ablauschen lässt. Laut den Sicherheitsexperten sind außer Intel-Prozessoren vermutlich auch andere mit Simultaneous Multi-Threading (SMT) betroffen, beispielsweise die von AMD.

Durch PortSmash gefährdet sind vor allem virtuelle Maschinen auf Cloud-Servern, die sich einen physischen Kern mit einer weiteren virtuellen Maschine teilen. Für OpenSSL gibt es bereits einen Patch gegen PortSmash. Der CVE-Eintrag (CVE-2018-5407) bewertet das Angriffsrisiko allerdings nur als „moderat" (CVSS v3: Score 4,8 von 10), weil eine Attacke sehr komplex ist. *(ciw@ct.de)*