CSCC Case der Woche

Potenzielle Schwachstellen in AMD-Prozessoren

Title

	Risiko ■■■□□
Sachstand:	Sicherheitsforscher der CTS-Labs haben 13 Schwachstellen in AMD-Prozessoren identifiziert. Die Schwachstellen werden in vier Kategorien eingegliedert und ermöglichen diverse Angriffsszenarien: **RYZENFALL**: Code Execution, Bypass des Windows Credential Guard **FALLOUT**: Installation von persistenter Schadsoftware **CHIMERA**: zwei Backdoors (Firmware, Hardware) **MASTERKEY**: BIOS-Flashing, Installation von persistenter Schadsoftware. Die Schwachstellen sind praktisch in allen aktuell verbreiteten AMD-Systemen enthalten (EPYC Server, RYZEN Workstation, RYZEN Pro, RYZEN Mobile).
Bewertung:	Die Medien stellen teilweise die Glaubhaftigkeit der Schwachstellen in Frage. Unter anderem wird dies dadurch begründet, dass die Firma CTS-Labs in der Security-Branche bisher unbekannt sei. Aus neutraler Sicht existieren im ersten Fall keine Beweggründe, von einer fälschlichen Sachlage auszugehen, zumal ein unabhängiger Dritter bereits einige der Schwachstellen bestätigt haben soll. Sollten die Schwachstellen seitens AMD bestätigt werden, hängt die Bedrohungslage zum einen von den aktuell noch unbekannten Angriffsvektoren und zum anderen von der Verbreitung der betroffenen Prozessoren statt. Naturgemäß wird die Situation mit Meltdown & Spectre verglichen, ein präziser Vergleich ist aufgrund noch nicht bekannten technischen Details aktuell nur schwer möglich.
Empfehlung:	Zurzeit können keinen konkreten Empfehlungen ausgesprochen werden. Die gemeldeten Schwachstellen liegen AMD zur Überprüfung vor. Die Lage sollte weiter beobachtet werden.
Quellen:	[1] Severe Security Advisory on AMD Processors

RISK