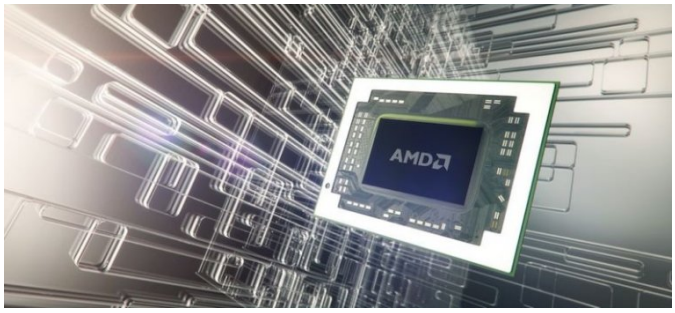
Israeli security firm CTS Labs announces the discovery of no less than 13 critical security vulnerabilities and manufacturer backdoors in AMD EPYC, Ryzen, Ryzen Pro and Ryzen Mobile processors.



The flaws potentially allow attackers to run malware that is not only nearly impossible to detect, but also provides direct access to the most (supposedly) secure part of the processor, namely the part storing sensitive data such as passwords and encryption keys. Taking advantage of most of the vulnerabilities does require administrative access, but they still allow a higher potential for damage than most regular attacks.

The CTS Labs report sorts the flaws into 4 categories-- Masterkey (allows attackers to infiltrate the Secure Processor, requires a re-flash of the BIOS with a specially crafted BIOS update), Ryzenfall (allows malicious code to completely take over the Secure Processor, requires attackers to run a program with local-machine elevated admin privileges), Fallout (allows attackers to read and write protected memory areas, such as SMRAM and Windows Credential Guard isolated memory, requires admin privileges) and Chimera (two backdoors, one in firmware and the other in hardware, accessible via driver digitally signed by the vendor).

The security firm says it has already shared all information with AMD, as well as partners Microsoft, HP, Dell and select security companies. However the report was released in an unusual manner, since CTS Labs did not give AMD the 90-day notice typically given when serious security flaws are discovered. Instead the report was published just 24 hours after AMD was first informed about it. This lead to critics suggesting it was been an attempt at influencing AMD stock prices.

"We find it unusual for a security firm to publish its research to the press without providing a reasonable amount of time for the company to investigate and address its findings," an AMD statement reads. "At AMD, security is a top priority and we are continually working to ensure the

safety of our users as potential new risks arise."

Whatever the reasons behind the way the report's release, a number of security researchers state the flaws are very real. Taking advantage of them is difficult, but admins should not ignore its warnings.

Go Severe Security Advisory on AMD Processors

Go The View from Our Corner of the Street