Threat Intelligence: Ryzen & EPYC

Published: Mar 15, 2018

Summary

In contrast to the customary 90+ day period given to semiconductor vendors to respond to vulnerabilities discovered by security researchers, as in the case of Meltdown & Spectre, CTS Labs announced 13 critical findings on March 15, 2018 that could leave select AMD processors compromised through potentially severe vulnerabilities and 24 hours for the manufacturer to respond prior to publishing their findings.

Impacted Systems include: AMD's EPYC server, Ryzen workstation, Ryzen Pro and Ryzen mobile chipsets. Currently 21 of AMD's chipsets have been successfully exploited.

Overview

Key Findings

- According to CTS Labs, the flaws are attributed to the architectural design of the AMD chipset's "Security Gatekeeper" and how it stores sensitive information, such as passwords, and can be categorized accordingly.
    - Chimera – Targets Ryzen workstation and Ryzen Pro chipsets and enables code injection techniques that leverage the Direct Memory Access engine to attack the operating system itself.
    - Ryzenfall – Targets AMD's Ryzen workstation, Pro and Mobile chipsets and allows malicious code to take complete control over the AMD Secure Processer and use its privileges to read and write to protected memory areas.
    - Fallout - Targets AMD's EPYC server chips and also allows attackers to read and write to and from protected memory areas.
    - Masterkey - This flaw consist of three separate vulnerabilities found in the manufacturer's firmware that allows malicious actors to infiltrate the Secure Processor in the EYPC server, Ryzen workstation, Ryzen Pro and Ryzen mobile chips and tamper with and bypass BIOS flashing protections.

Mitigation

1. CTS Labs, after discussing the vulnerabilities with manufacturers and other security experts, speculated that AMD would not be able to fix the vulnerabilities for "many, many months, or even a year." Instead of waiting to reveal these vulnerabilities, CTS Labs decided to inform the public of its discovery.

2. AMD's response: "We have just received a report from a company called CTS Labs claiming there are potential security vulnerabilities related to certain of our processors. We are actively investigating and analyzing its findings. This company was previously unknown to AMD and 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. At AMD, security is a top priority and we are continually working to ensure the safety of our users as potential new risks arise."

NOTE: Currently, there are no known mitigations. AMD has recently released a BIOS update that purportedly allows users to disable the "Secure Processor." However, this feature does not address the RYZENFALL attack method.

The vulnerabilities could be potentially useful to attackers at different stages of an Advanced Persistent Threat (APT) attack against an enterprise network, despite requiring admin privileges to exploit it:

1. Persistency: Attackers could load malware into the AMD Secure Processor before the CPU starts. From this position, they can prevent further BIOS updates and remain hidden from security products.

2. Stealth: Sitting inside the AMD Secure Processor or the AMD Chipset is, at the moment, outside the reach of virtually all security products. AMD chips could become a safe haven for attackers to operate from.

3. Network Credential Theft: Bypass Microsoft Credentials Guard and steal network credentials. For example, a PoC version of mimikatz that works even while Credential Guard is enabled.

4. Specific AMD Secure Processor features for cloud providers, such as Secure Encrypted Virtualization, could be circumvented or disabled by these vulnerabilities.

Further Reading

https://safefirmware.com/Whitepaper+Clarification.pdf
https://safefirmware.com/amdflaws_whitepaper.pdf
https://amdflaws.com/