CTS-LABS RESPONSE TO AMD'S INITIAL ASSESSMENT OF VULNERABILITIES

- **We believe AMD is attempting to downplay the significance of the vulnerabilities**
- **Our view is AMD's suggested timeline for its patches roll out is drastically optimistic – we believe a number of the fixes are likely to take months, not weeks**
- **We believe the AMD flaws have potential to turn a local problem into a network-wide problem**
- **Notably, AMD did not provide a time estimate for patching CHIMERA**

On March 12, CTS-Labs ("CTS") reported to AMD 13 severe vulnerabilities in AMD processors that we believe are onerous to fix. AMD yesterday confirmed the existence of these vulnerabilities, but disputes how time-consuming and difficult it will be to fix them.

Our view is that AMD is attempting to downplay the significance of its vulnerabilities by emphasizing that they require local administrative access. Let us be clear: AMD's argument that administrative access "effectively grants the user unrestricted access to the system" is factually false and contradicts the company's own past statements. If administrative access grants users complete access to the system, then why did AMD design and implement security measures such as the Secure Processor? In fact, isolation of secure information from admin-privilege users is a central design idea behind the Secure Processor.

As AMD's own Security Architect David Kaplan explained in his 2016 lecture at the Linux Security Summit, a feature of the Secure Processor called Secure Encrypted Virtualization was specifically designed to prevent rogue cloud administrators, obviously in possession of administrative privileges, from being able to access customer data. This is a fundamental concept that needs to be paid further attention, and AMD should be challenged on it.

Attackers think of computers as nodes in a network. Successful cyber-attacks always begin with a complete compromise of a single computer which includes local administrative access. Phishing attacks are routinely successful in modern organizations. The challenge for attackers is then to spread out into other computers. This is exactly what the AMD vulnerabilities provide by allowing Windows Credential Guard to be bypassed.

AMD's flaws turn a local problem into a network-wide problem. Furthermore, once attackers have reached an AMD machine, they can become entrenched there beyond the reach of almost all security products, likely forcing a CISO to physically remove that machine from the network.

We firmly believe that AMD's suggested roll-out timeline for its patches is also drastically optimistic. In our view, any change in the Secure Processor firmware must undergo two consecutive layers of integration and Quality Assurance (QA). First, the patching must pass AMD's own QA. Second, it must be transferred over to the OEMs for OEM-specific QA for every product that includes affected AMD processors. In the case of the Ryzen chipset affected by CHIMERA, there is yet another layer of QA for ASMedia -- the IP provider.

Notably, AMD did not provide a time estimate for patching CHIMERA. This vulnerability includes two sets of manufacturer backdoors on Ryzen chipsets identified by CTS, one of which is scorched into the

hardware itself -- implemented in ASIC and fabricated into the chip. These backdoors cannot be physically removed and would require either a complicated workaround or hardware replacement. We therefore believe that AMD's unrealistic estimate that it will take "weeks" to deliver the patches to AMD customers will be proven false. Time will tell, but we see a timeline where 'weeks' could turn into months.

Furthermore, the manufacturer backdoors left in its Ryzen and Ryzen Pro chipsets – a central motherboard component – portray, in our opinion, a level of neglect that is reminiscent of the late 1990s. This raises questions about whether this IP was audited before integration.

In addition, it appears that the chipset and the Secure Processor are missing industry standard mitigations against exploitation such as Stack Canaries. The lack of such mitigations makes it exceedingly easy for attackers to exploit security vulnerabilities once they are discovered.

If AMD customers had the capability to disable the Secure Processor by severing its communications interface with the main processor, as advertised in the description of the recently released "Disable PSP" feature, this would have provided AMD customers with a solution against at least some of the vulnerabilities. Currently, the feature only disables the fTPM, while leaving the vulnerabilities exploitable.

Finally, and perhaps most concerning of all, is the fact that six security researchers, albeit highly experienced, managed to identify 13 distinct security vulnerabilities in the flagship products of an $11B company with comparably infinite budget for security, and over a period of only six months.

Regardless of views on how we communicated the information, the fact remains that this further raises a red flag about the overall state of affairs in AMD Product Security.