CTS LABS SEEKS UPDATE ON AMD'S SUPPOSED PATCH ROLLOUT TIMELINE

- As predicted, AMD's optimistic timeline to roll out patches for MASTERKEY, RYZENFALL and FALLOUT has proven false
- Almost six weeks following their statement promising fixes in the "coming weeks", not a single patch has been provided
- There is still no projected timeline for CHIMERA, whose hardware vulnerabilities will require a workaround
- AMD has encrypted portions of its PSP firmware. However, this '*Security by Obscurity'* does not fix any of the vulnerabilities CTS discovered.

May 1, 2018 -- We are closing in on six weeks from AMD's technical assessment of our research on March 21. Following this initial assessment, we released a statement with our view that AMD was attempting to downplay the significance of the vulnerabilities we found, as well as the fact that AMD's suggested timeline for its patches roll out was drastically optimistic; https://bit.ly/2FtyweR

As we approach the six week mark, we believe our views are being validated and stand by our conviction that a number of the 13 vulnerabilities will indeed take many months to fix.

"Despite AMD promising to release PSP firmware patches for MASTERKEY, RYZENFALL and FALLOUT within 'the coming weeks', no patches have been released," said Ido Li On, CEO of CTS. "Not only have no patches been rolled out, there have been no updates or communication from AMD on progress, or on when these patches can be expected. Furthermore, as we pointed out in our previous statement, not so much as a projected timeline has yet been provided for CHIMERA."

According to CTS' assessment, as well as the assessment of experts the firm has consulted with, firmware vulnerabilities such as MASTERKEY, RYZENFALL and FALLOUT could take several months to fix. Hardware vulnerabilities such as CHIMERA cannot be directly fixed and require a workaround.

In an update released on April 14, AMD encrypted portions of its PSP firmware. "This is going to prevent researchers from auditing AMD's firmware, or even from validating AMD's patches. It is basically security through obscurity," says Uri Farkas, CTS VP R&D.

As rightly worded by Wikipedia: "security by obscurity is discouraged and not recommended by standards bodies. The National Institute of Standards and Technology (NIST) in the United States specifically recommends against this practice… system security should not depend on the secrecy of the implementation or its components."

"Since questions on security were almost non-existent on AMD's recent earnings call, and no one else is challenging AMD on their nonchalance about the patching process, we are more than happy to ask the question and look forward to an update," said Yaron Luk-Zilberman, CTS CFO.

###