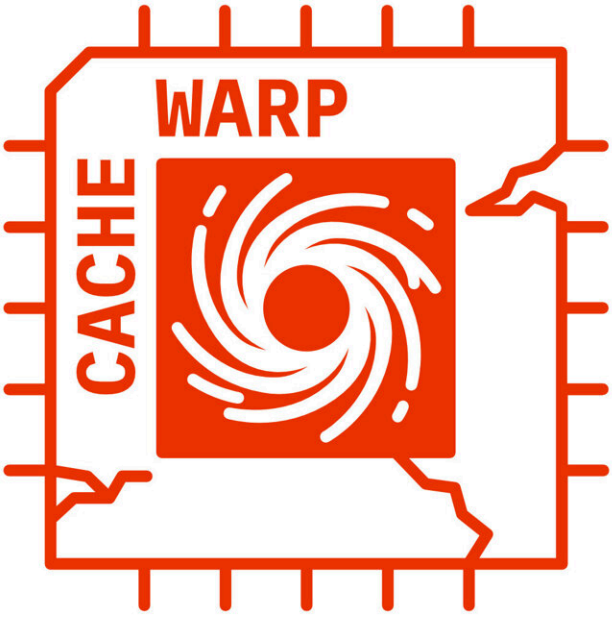
New CPU vulnerability extends to virtual machine environments

November 14 2023, by Falko Schoklitsch



The security vulnerability CacheWarp poses a risk for virtual machines based on AMD processors. Credit: CISPA

In the area of cloud computing—on-demand access to IT resources via the internet—so-called trusted execution environments (TEEs) play a major role. They are designed to ensure that the data on the virtual work environments (virtual machines) is secure and cannot be manipulated or stolen.

Researchers at the CISPA Helmholtz Centre for Information Security and Graz University of Technology (TU Graz) have now discovered a security vulnerability in AMD processors that allows attackers to penetrate virtual work environments based on the trusted computing technologies AMD SEV-ES and AMD SEV-SNP. This is achieved by resetting data changes in the buffer memory (cache), which gives the intruders unrestricted access to the system. They have chosen CacheWarp as the name for this software-based attack method.

The research team, led by Michael Schwarz from the CISPA Helmholtz Centre for Information Security, has created its own website to provide information on CacheWarp. The scientific paper titled "CacheWarp: Software-based fault injection using selective state reset" is available on the site and has already been accepted for the USENIX Security conference 2024.

CacheWarp turns back time in memory

AMD Secure Encrypted Virtualization (SEV) is a processor extension that provides secure separation between virtual machines and the underlying software, known as the hypervisor, for managing the required resources. AMD SEV encrypts the data on the virtual machine for this purpose. CacheWarp can be used to undo data modifications in this working environment and fool the system into believing it has an outdated status. This is problematic, for example, if a variable determines whether a user is successfully authenticated or not.

Successful authentication is usually marked with "0," which is the same value with which the variable is initialized. If a potential attacker enters an incorrect password, the variable is overwritten with a value not equal to "0." However, CacheWarp can be used to reset this variable to its initial status when it indicated successful authentication. This allows an attacker to establish an already authenticated session.

This is made possible by an unexpected interaction between CPU instructions and AMD SEV, through which the cache can be reset to its old state. Once the attacker has gained access in this way, they can subsequently gain the full access rights of an administrator to the data in the virtual machine. During their tests, the researchers were able to take all the data located there, modify it and spread from the virtual machine further into the user's infrastructure. They first bypassed the secure login and then overcame the barrier between normal user and administrator.

AMD provides update

As is usual in such cases, the researchers informed the manufacturer concerned—in this case AMD—about the security vulnerability in advance so that it could take the necessary measures before the research results are published. AMD has identified CacheWarp under the identifier CVE-2023-20592 and is providing a microcode update that fixes the vulnerability. The manufacturer has published further information on this in the AMD Security Bulletin.

"Research in the field of microarchitectural attacks is fascinating because it very often reveals just how complex our modern computer systems have become," says Andreas Kogler from the Institute of Applied Information Processing and Communications (IAIK) at TU Graz.

"It's amazing how the interplay of several factors makes it possible to extract or change data from such systems. Our work on CacheWarp shows how an attacker can make write accesses to the memory of the affected processors virtually forgotten. You can think of it like older USB sticks. If you overwrote a document there, but removed the stick before the end of the writing process, you could find parts of the old version instead of the new one the next time you plugged in and read the document."

Paper authors are Ruiyi Zhang, Lukas Gerlach, Daniel Weber, Lorenz Hetterich, Michael Schwarz (all CISPA Helmholtz Centre for Information Security); Andreas Kogler (TU Graz) and Youheng Lü (independent).

More information: Ruiyi Zhang et al, CacheWarp: Software-based fault injection using selective state reset (2023).

Provided by Graz University of Technology