- Risk Management
- Compliance
- Privacy
- Supply Chain

- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › Vulnerabilities

Voltage Glitching Attack on AMD Chips Poses Risk to Cloud Environments

By Eduard Kovacs on August 13, 2021

Researchers have described a voltage glitching attack that shows AMD's Secure Encrypted Virtualization (SEV) technology may not provide proper protection for confidential data in cloud environments.

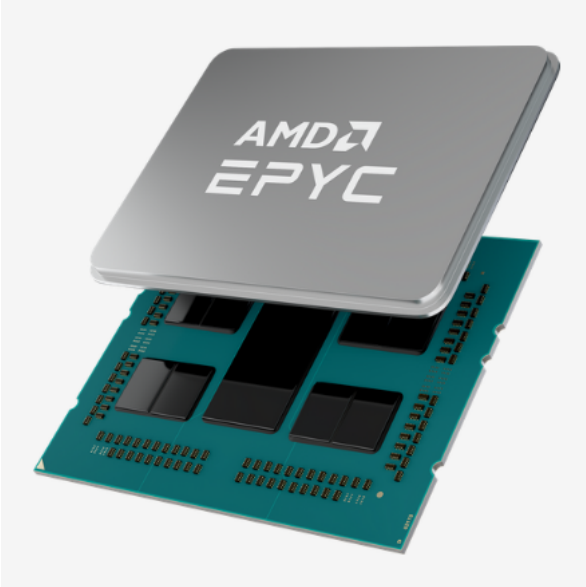
The research was conducted by a team from the Technical University of Berlin (TU Berlin) and it was detailed in a paper published this week.

AMD's SEV technology — present in the company's EPYC processors — is designed to protect virtual machines (VMs) and the data they store against insider threats with elevated privileges, such as a malicious administrator. SEV is often used in cloud environments.

SEV is designed to protect confidential data by encrypting the VM's memory, and the encryption keys are secured using AMD's Secure Processor (SP), a dedicated security co-processor. This should ensure that only the SP has access to the memory encryption key, while the hypervisor, which can be under the control of a threat actor, does not.

However, the TU Berlin researchers showed that an attacker who has physical access to the targeted system can gain access to SEV-protected VM memory content by launching a voltage fault injection attack on SP.

In order to work as intended, integrated circuits need to operate within specific temperature, clock stability, electromagnetic field, and supply voltage ranges. Purposefully manipulating one of these parameters is called a glitching attack. Such attacks require physical access to the chip, but they can be useful for obtaining sensitive information, bypassing security checks, or achieving arbitrary code execution.



In their voltage glitching attack, the researchers showed that by manipulating the input voltage to AMD chips, they can induce an error in the ROM bootloader of the SP, allowing them to gain full control. They described the risk posed to cloud environments due to SEV's failure to properly protect potentially sensitive information from malicious insiders.

"We presented how an adversary with physical access to the target host can implant a custom SEV firmware that decrypts a VM's memory using SEV's debug API calls," the researchers explained in their paper. "Furthermore, we showed that the glitching attack enables the extraction of endorsement keys. The endorsement keys play a central role in the remote attestation mechanism of SEV and can be used to mount remote attacks. Even an attacker without physical access to the target host can use extracted endorsement keys to attack SEV-protected VMs. By faking attestation reports, an attacker can pose as a valid target for VM migration to gain access to a VM's data."

The hardware needed to conduct such an attack is widely available and inexpensive, but the researchers said it took them 4 hours to prepare a system for an attack, which significantly lowers the risk in a real world environment.

While this is not the first research project focusing on voltage glitching attacks or attacks on AMD's SP and SEV, the researchers said that — to the best of their knowledge — this is the first attack affecting all AMD EPYC CPUs (Zen 1, Zen 2 and Zen 3).

The researchers have reported their findings to AMD and proposed some mitigations that could be implemented in future CPUs.

SecurityWeek has reached out to AMD for comment and will update this article if the company responds.

**updated to clarify that it took the researchers 4 hours to prepare a system for an attack*

Related: PLATYPUS: Hackers Can Obtain Crypto Keys by Monitoring CPU Power Consumption

Related: VoltPillager: New Hardware-Based Voltage Manipulation Attack Against Intel SGX

Related: Plundervolt Attack Uses Voltage to Steal Data From Intel Chips

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia' s security news reporter. Eduard holds a bachelor' s degree in industrial informatics and a master' s degree in computer techniques applied in electrical engineering.
Previous Columns by Eduard Kovacs: