Glossary of Terms

ABL	AMD Boot Loader
AES	Advanced Encryption Standard
AMD SMM Supervisor	A security module that helps isolate SMM
APCB	AMD ASP Configuration Block
ASP	AMD Secure Processor, a microcontroller within the AMD processor that handles security and boot time tasks. (Formerly referred to as PSP)
Authenticated	Privileges are low: User needs to log in but level of privileges are low - No root access, no admin access, no super user, etc. required. (e.g.: Guest VM)
DMA	Direct Memory Access
DRTM	Dynamic Root of Trust for Measurement
Gadget	A gadget is a snippet of pre-existing code that is typically found through reverse engineering.
HV	Hypervisor
INVD	Invalidates/flushes a processor's internal caches and issues a special-function bus cycle that directs external caches to also flush themselves.
IOCTL	Input Output Control
IOMMU	I/O memory management unit
MA	Migration Agent
MMIO	Memory Mapped I/O
MSR	Model Specific Register (Click here for more information, p.59)
PF	Physical function
PMFW	Power Management Firmware
Privileged	Privileges required: High Admin, Root, Super Use privileges, hypervisor privileges required.
PSP	AMD Platform Security Processor, a microcontroller with the AMD processor that handles security and boot time tasks. (See ASP)
RDRAND	A hardware-based random number generation instruction in x86 processors that provides a cryptographically secure random number for use in tasks such as generating encryption keys and establishing secure network connections.
RMP	Reverse Map Paging
ROM	Read Only Memory
S3	S3 is a special boot flow as defined by the ACPI (Advanced Configuration and Power Interface) specification.
SEV	AMD Secure Encrypted Virtualization feature
SEV-ES TMR	Trusted Memory Region set up during SEV-ES Initialization to protect the Virtual Machine Save Areas
SMI	System Management Interrupt
SMM	x86 System Management Mode, a highly privileged execution mode used by the platform BIOS.
SMN	System Management Network
SMRAM	System Management RAM. A portion of the systems memory used by the processor to store code used with SMM.

SMT	Simultaneous Multi-Threading
SMU	AMD System Management Unit, a microcontroller within the AMD processor that handles real-time events such as power management.
SNP	AMD Secure Nested Paging feature
SPA	System Physical Address
SPI ROM	Serial Peripheral Interconnect Read-Only Memory. A small storage device soldered to a motherboard that contains the platforms boot code, including the AMD firmware components, and the systems BIOS.
TA	Trusted Application
TEE	Trusted Execution Environment
TLB	Translation Lookaside Buffer
TMR	Trusted Memory Region (see SEV-ES TMR)
TOCTOU	Time-Of-Check to Time-Of-Use
TPM	Trusted Platform Module.
TSC	Time Stamp Counter (Click here for more information. P.422)
UApp	User Application
UEFI	Unified Extensible Firmware Interface
Unauthenticated	Privileges required: None. Log in not required- can run the exploit on devices with zero credentials.
Unprivileged	For programs that allow “unprivileged” access modes. (e.g: user space vs kernel, SMM vs PSP).
Use-After-Free	Please see the link for a detailed description from CWE: https://cwe.mitre.org/data/definitions/416.html
VM	Virtual Machine
VMSA	Virtual machine Save Area (Click here for more information. P.15)
VMCB	Virtual Machine Control Block