海光处理器免疫 StackWarp 漏洞的说明

目录

1. StackWarp 漏洞介绍

德国 CISPA 亥姆霍兹信息安全中心的研究人员披露了 StackWarp 漏洞，并在《StackWarp: Breaking AMD SEV-SNP Integrity via Deterministic Stack-Pointer Manipulation through the CPU's Stack Engine》[1]论文中描述了漏洞细节，漏洞编号为 CVE-2025-29943。

StackWarp 是一种主机侧通过修改特定 MSR 寄存器、结合单步执行机制[2]，突破 AMD SEV-SNP 虚拟机完整性保护的漏洞。AMD SEV-SNP 虚拟机以主机不可信任为安全模型。StackWarp 漏洞通过主机更改 MSR 0xC001102E 的 bit 19 使得虚拟机 RSP 寄存器的值更新发生异常。由于虚拟机程序栈中保存了函数返回地址和程序运行数据，攻击者可通过篡改虚拟机 RSP 寄存器，实现虚拟机程序执行控制流和数据流篡改。攻击者可以利用 SEV-SNP 虚拟机单步执行机制在虚拟机特定指令处退出到 Host 实施精确攻击，因而通过该漏洞可以实现符合意图的攻击，例如 RSA 秘钥恢复、绕过 OpenSSH 的密码认证等。

2. AMD 的防御措施

AMD 漏洞公告[3]描述了通过更新 Platform Initialization (PI) firmware 修复该漏洞的防御措施。

3. 海光处理器的免疫状态

该漏洞针对的是 AMD SEV-SNP 新一代的加密虚拟化技术，海光处理器不存在该漏洞所针对的 AMD SEV-SNP 技术，所以海光处理器对该漏洞免疫。

海光加密虚拟化技术即 CSV3 是海光完全自主研发的虚拟化技术，其硬件实现和 AMD 的 SEV-SNP 虚拟化技术存在本质区别，海光 CSV3 技术不存在该漏洞利用的条件，因此海光处理器 CSV3 技术也免疫该漏洞攻击。

具体来说，该漏洞被用来实现有意义攻击的条件是在虚拟机的特定指令处退出到 Host 中篡改 MSR，而实现这一条件的关键前提是主机具备更改虚拟机页表从而能够构造虚拟机单步执行[2]的能力。AMD SEV-SNP 虚拟机的主机可以更改 NPT 页表，因此其主机具备虚拟机单步执行能力。海光 CSV3 技术能够阻止主机篡改 CSV3 虚拟机的页表，避免 SEV-SNP 虚拟机存在的单步执行的问题。攻击者在无法构造虚拟机单步执行的条件下，仅通过篡改 MSR 并不能在精确的指令处实现符合目的的攻击，因而海光 CSV3 技术可以阻止该漏洞的攻击。

综上所述，海光处理器对 StackWarp 漏洞免疫，海光处理器不受该漏洞攻击影响。

4. 参考

1. https://stackwarpattack.com/stackwarp_usenix26.pdf
2. L. Wilke, J. Wichelmann, A. Rabich, and T. Eisenbarth, “Sev-step: A single-stepping framework for amd-sev,” IACR Trans. Cryptogr. Hardw. Embed. Syst., 2024.
3. https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3027.html