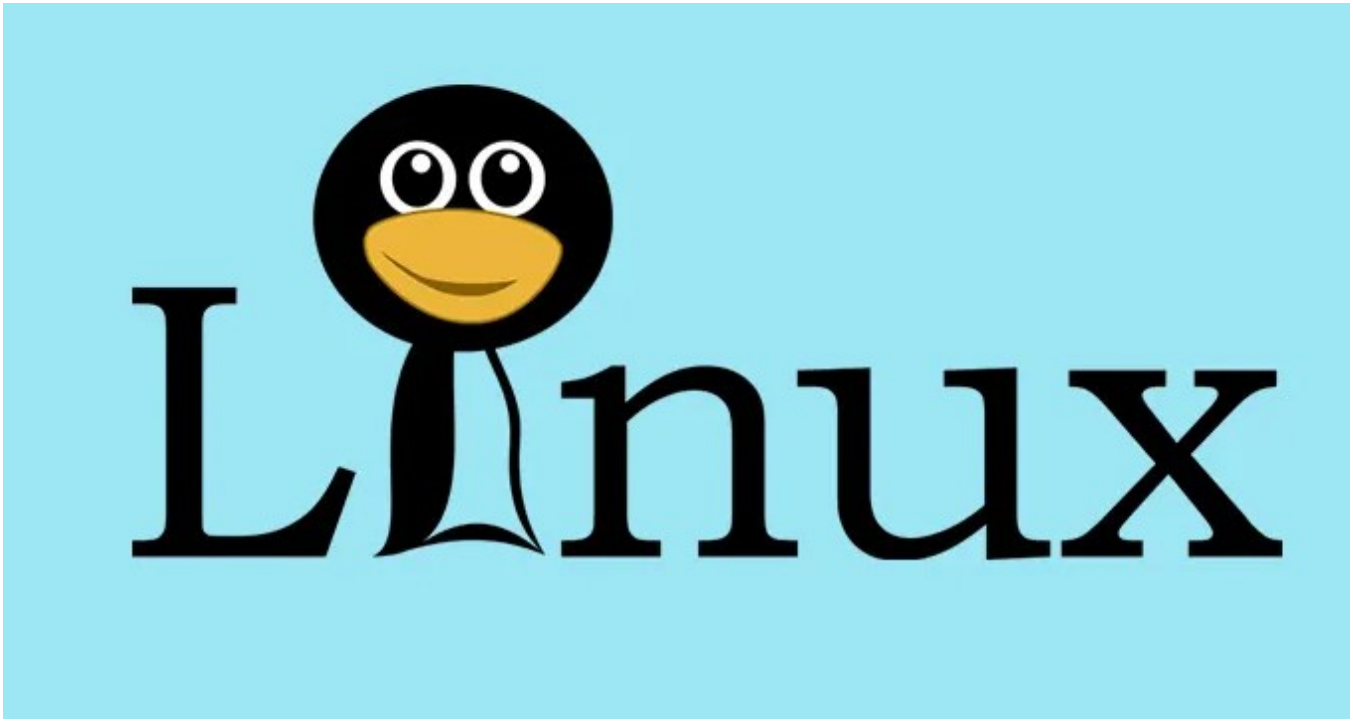
Linux 6.2增强硬件安全

12月15日Linux 6.2最新消息，Linux 6.2增强硬件安全，正在开发状态下的Linux 6.2 在引入 TDX 访客认证支持之外，还计划为英特尔的英特尔软件防护扩展（SGX）引入异步退出通知（Asynchronous Exit Notification）机制。



Linux 6.2 内核合并的最新 SGX 代码，可以安全地使用新英特尔 CPU 的异步退出（AEX）通知机制。AEX 通知路径允许在退出事件上运行一个处理程序，这反过来又可以缓解 SGX-Step 漏洞等问题。对 AEX Notify 的支持有助于加强英特尔 SGX 周围的防御，以防止整类攻击。

随着现在 Linux 6.2 中 x86 / sgx 代码的合并，AEX Notify 支持在裸机（Bare-metal）用户空间运行环境（enclave）和 KVM 虚拟机（VM）中使用，以更好地保护支持处理器上的 SGX 用户空间运行环境。

除了 SGX AEX Notify 和 TDX 客体认证，Linux 6.2 的其它安全改进还包括用于降低 Skylake 时代处理器 Retbleed 开销的 Call Depth Tracking，FineIBT 作为支持间接分支跟踪（IBT）的 CPU 的控制流完整性选项，以及常规的安全改进。

英特尔软件防护扩展是一组安全相关的指令，它被内置于一些现代 Intel 中央处理器中。它们允许用户态及内核态代码定义将特定内存区域，设置为私有区域，此区域也被称作飞地。其内容受到保护，不能被本身以外的任何进程存取，包括以更高权限级别运行的进程。CPU 对受 SGX 保护的内存进行加密处理。

本文链接：https://dqcm.net/zixun/16710940773325.html