

USN-4901-1: Linux kernel (Trusty HWE) vulnerabilities

Adam Nichols discovered that heap overflows existed in the iSCSI subsystem in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-27365)

It was discovered that the LIO SCSI target implementation in the Linux kernel performed insufficient identifier checking in certain XCOPY requests. An attacker with access to at least one LUN in a multiple backstore environment could use this to expose sensitive information or modify data. (CVE-2020-28374)

Adam Nichols discovered that the iSCSI subsystem in the Linux kernel did not properly restrict access to iSCSI transport handles. A local attacker could use this to cause a denial of service or expose sensitive information (kernel pointer addresses). (CVE-2021-27363)

Adam Nichols discovered that an out-of-bounds read existed in the iSCSI subsystem in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information (kernel memory). (CVE-2021-27364)