|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S.no** | **Threat Event(s)** | | **Vulnerabilities** | | **Security risk level** | |
| Precession knee | Intra-Op |
| 1 | T02 | Deliver directed malware | V02 | Ineffective management of admin credentials | Medium | Low |
| 2 | T03 | Perform perimeter network reconnaissance/scanning | V21 | Unprotected network port | Low | Low |
| 3 | T05 | Conduct scavenging of ePHI at rest | V01 | Ineffective management of user credentials | Medium | Low |
| 4 | T05 | Conduct scavenging of ePHI at rest | V04 | Unauthorized modification to system bios | Medium | Low |
| 5 | T06 | Theft of system or hard drives | V24 | Any unprotected hardware | Medium | Low |
| 6 | T07 | Data theft via physical media | V22 | Unprotected external USB Port | Low | Low |
| 7 | T08 | Network-based denial of service (DoS) attack | V21 | Unprotected network port | Medium | Low |
| 8 | T10 | Mis-configuration by user | V03 | Untrained/Malicious User | Low | Low |
| 9 | T11 | Remote exploitation | V21 | Unprotected network port | Medium | Low |
| 10 | T11 | Remote exploitation | V21 | Unprotected network port | Medium | Low |
| 11 | T12 | Improper disposal of hard disks | V24 | Any unprotected hardware | Low | Low |
| 12 | T13 | Man-in-the middle attack / intercept Navigation communication | V24 | Any unprotected hardware | Medium | Low |
| 13 | T16 | Physical Manipulation of Hardware | V24 | Any unprotected hardware | Medium | Low |
| 14 | T16 | Physical Manipulation of Hardware | V24 | Any unprotected hardware | Medium | Low |
| 15 | T21 | Power Failure at primary facility | V24 | Any unprotected hardware | Low | Low |
| 16 | T24 | Manipulation of navigation camera firmware / memory | V24 | Any unprotected hardware | Medium | Low |