1. Total “**Medium risk level**” in Precession Knee: **16**
2. **Medium** in Precession Knee & **Low** in Intra-Op: **12**
3. **Medium** in Precession Knee & **Medium** in Intra-Op: **1**
4. **Medium** in Precession Knee & **not existed** in Intra-Op: **3**
5. Total “**Medium risk level”** in Intra-Op: **53**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **Medium Risk level list**  **Precession Knee** |  |  |  |  | **Intra-Op**  **Risk level** |
| 1 | T02 | Deliver directed malware | V24 | Unprotected hardware | A01 | System resources | - |
| 2 | T05 | Conduct scavenging of ePHI at rest | V01 | Ineffective management of user credentials | A05 | Patient health information at rest | Low |
| 3 | T02 | Deliver directed malware | v02 | Ineffective management of admin credentials | A02 | Admin Password / Credentials / System Configuration / Certificates | Low |
| 4 | T13 | Man-in-the middle attack / intercept Navigation communication | V24 | Unprotected hardware | A09 | Navigation Accuracy | Low |
| 5 | T08 | Network-based denial of service (DoS) attack | V21 | Unprotected network port | A01 | System resources | Low |
| 6 | T11 | Remote exploit | V21 | Unprotected network port | A09 | Navigation Accuracy | Low |
| 7 | T11 | Remote exploit | V21 | Unprotected network port | A01 | System resources | Low |
| 8 | T06 | Theft of system or hard drives | V24 | Unprotected hardware | A01 | System resources | Low |
| 9 | T16 | Physical Manipulation of Hardware | V24 | Unprotected hardware | A02 | Admin Password / Credentials / System Configuration / Certificates | Low |
| 10 | T17 | Gather information using open source discovery of organizational information | V21 | Unprotected network port | A01 | System resources | - |
| 11 | T01 | Deliver undirected malware | V13 | Defect or bug in Stryker software | A01 | System resources | Medium |
| 12 | T05 | Conduct scavenging of ePHI at rest | V04 | Insecure Boot / Boot for external media | A05 | Patient health information at rest | Low |
| 13 | T24 | Manipulation of navigation camera firmware / memory | V24 | Unprotected hardware | A09 | Navigation Accuracy | Low |
| 14 | T16 | Physical Manipulation of Hardware | V24 | Unprotected hardware | A09 | Navigation Accuracy | Low |
| 15 | T01 | Deliver undirected malware | V11 | Unpatched COTS operating system | A01 | System resources | - |
| 16 | T11 | Remote exploit | V11 | Unpatched COTS operating system | A02 | Admin Password / Credentials / System Configuration / Certificates | Low |