System/cart: Nav 3/3i

OS: Windows 8.1

App: Intra-op

|  |  |  |  |
| --- | --- | --- | --- |
| Attack vector | Risk | Mitigation | Recommendation |
| 1.Outdated OS  (Windows 8.1) | For an EOL OS, Vulnerability addressing & Patch Updates are not available to protect Nav 3/3i. | **From the OS**:  For Business Continuity if there is a need to stick with Windows 8.1 for Nav3/3i , Additional protection measures needs to be designed. | Perform an Audit to find out the Vulnerable areas and attack surfaces.  OS perspective protection measures needs to be addressed in Nav 3/3i carts. |
| 2. Unsupported OEM tools (such as Microsoft Defender) | For OS Security Tools used in Nav3i cart, updates are not available from OEM. | **From the OS**:  For the EOL OS, all the OEM tools to be replaced with the alternate supporting tools. | Alternate software tools needs to be identified and updated in Nav3/3i cart. |
| 3. External/Internet Access | Getting exposed to malicious/untrusted external sources | **From the OS**:  No network services should be provided by the Nav 3/3i cart | Disable the modules & services for internet access in windows 8.1. |
| 4.Outdated virus definitions  (with Microsoft Defender) | with outdated virus definitions, virus/malware can stay unidentified and affect the system. | **From the OS**:  Replace the tool (Windows Defender) with the tool that provides Updated virus definitions for Nav3i EOL OS | Update the outdated antivirus with latest virus definitions |
| 5. Remote Access | High possibility of network attacks using different Remote Desktop software tools by adversary in Nav3i  (ex: MITM) | **From the OS**:  Remove the OS services providing the RDP protocol and support | Provide local support to Cart. Service person should visit the hospital to provide the necessary support |
| 6. Application Filtering | Every application gets installed & accessed in the same way. There is no priority/privilege in Nav3i | **From the OS**: Whitelisting (Applocker) needs to be checked for the applications. | All applications should not be treated with same priority/privilege |
| 7. Unused/Unnecessary binaries, drivers, services, ports & protocols | It provides info about the system internals and often found vulnerable to attack | **From the OS**:  List out all the unused/unnecessary binaries, drivers, services, ports & protocols and disable them | Remove the binaries, drivers, services, protocols & ports that are not used/required |
| 8. Lack of authentication for the connected removable device | If authentication is not enabled, any removable device can be connected to the cart and trust can't be established | **From the OS:**  ‘On Access’ scan should be validated for the windows 8.1 Nav3i and ensure latest virus definitions are present | Authentication of input device and Virus scan with latest definitions are mandatory. |
| 9. Data restoration/Backup | Due to any abnormal activity occurred in OS, patient/case data gets lost and then without backup plan implemented, Apps can't restore to the previous state after the abnormal activity | **From the OS** :  For Cart OS, planning Restore points are mandatory in EOL OS  **From the App**:  Apps need to plan their own Backup provided for OS related application components  (ex: dll file) | Application should adapt the data backup policy. Data must be encrypted and stored in a secure location at periodic timeline intervals |
| 10. Insufficient key lengths | Weak encryption algos and Key lengths can be vulnerable to attack when an insufficient key length is used in EOL OS | **From the application**: Use appropriate stronger algos and key lengths in EOL OS. | Maximum key size/lengths and strong crypto algos supported by the windows 8.1 should be used. Weak and vulnerable by history needs to be avoided. |