System/cart: Nav 3/3i

OS: Windows 8.1

App: Intra-op

|  |  |  |  |
| --- | --- | --- | --- |
| Attack vector | Risk | Mitigation | Recommendation |
| Outdated OS  (Windows 8.1) | As an EOL OS vulnerability addressing & patch management are not available | From the OS: For business continuity stick with 8.1 with additional protection measures |  |
| Unsupported OEM tools (such as Microsoft Defender) | For anti-virus, updated virus definitions won’t get from OEM | From the OS: For the EOL OS all the OEM tools needs to be replaced with the alternative supporting tools | Alternate software needs to be found and updated |
| Internet Access | Possibility of accessing malicious/untrusted external sources | From the application: No network services should be provided by the Nav 3/3i cart | Disable the modules & services for internet access in windows 8.1. |
| Outdated virus definitions | If outdated virus definitions are present, virus/malware can easily affect the system | From the OS: Update the outdated virus definitions | Update the outdated virus definitions |
| Remote Access | High possibility of network attacks (ex: MITM) | From the application: Remove the Remote Desktop support | Provide local support. Service person should visit the hospital to provide the necessary support |
| Application Filtering | Every application gets installed & treated in the same way. There is no priority/privilege | From the OS: Whitelisting needs to be performed for the applications | All applications should not treated with same priority/privilege |
| 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 |
| Outdated/Weak/Insufficient crypto algos strength | Outdated cryptographic algorithms should be avoided to improve the attack complexity, as this can be easily cracked by the adversary | From the application: Outdated/Weak crypto algorithms need to be identified and removed | Latest & strong crypto algorithms should be selected for ensuring proper security |
| Unencrypted sensitive data | Info leakage might occur for unencrypted sensitive data (Crypto & PHI) existing in the cart | From the OS & Application:  Encryption/cryptographic techniques are important in securing the sensitive data | All sensitive data should be encrypted |
| 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: All the removable devices should not be allowed to connect with the system | Authentication of input device is mandatory |
| Data restoration/Backup | Due to any abnormal activity occurred in OS, application lost the patient/case data then without backup plan implemented can't restore to the previous state after the abnormal activity | From the : Backup should be 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 |
| Absence of data validation | Deviation from the desired input data affects functionality and also creates major risk to patient health during surgery | From the application: Format and length of the input data should be properly validated before being accepted by the application | Application should validate the input data. Data format and expected input should be properly documented |
| Insufficient key lengths | Strong encryption algos can be vulnerable to attack when an insufficient key length is used | From the application: Use appropriate algos and key lengths | Maximum key size/lengths supported by the windows 8.1 should be used |