Vulnerabilities	Category
Broken Authentication	Application
Buffer Overflow	Application
Data Inconsistency	Application
Insecure Access Management	Application
Insecure Interface Configuration	Application
Insecure Management of Data	Application
Insecure Software	Application
Lack of Active Device Monitoring	Application
Lack of Standardization	Application
Low Quality Level Code	Application
Non-repudiation	Application
SQL Injections	Application
Weak/lack In-app Encryption	Application
Malicious code in-app	Application
Systems Low-cost	Device
Channel Voice	Device
Default Configuration	Device
Device Spoofing	Device
Electromagnetic Emanations Leaking	Device
Energy Restraints	Device
Heterogeneous Interaction	Device
Insecure Data Transfer and Storage	Device
Insecure Firmware	Device
Insecure Initialization	Device
Insecure Password	Device
Insufficient Testing	Device
Lack of Side Channel Protection	Device
Lack of Strong Authentication	Device
Low Computing Power	Device
Low Data Transmission Range	Device
Malicious Code Injection	Device
Obtaining Console Access	Device
Physical Damage	Device
Physical Tampering	Device
Sleep Deprivation	Device
Tag Cloning	Device
Unprotected Physical Access	Device
Weak Access Control	Device
Weak/leak of Encrypt	Device
Insecure physical interface	Device
Channel Interference	Network
Communication Overhead	Network
Data Leak or Breach	Network
Denial of Service	Network
Eavesdropping	Network

Fake/Malicious Node	Network
Heterogeneous Communication	Network
Insecure Server	Network
Insecure Update Mechanisms	Network
Lack of Proper Authenticatication Mechanisms	Network
Lack of Strong Password	Network
Lack Secure Communication Protocols	Network
Configure network repeatedly	Network
Single-Point Dependency	Network
Spoofing Signal	Network
Unauthorized Access	Network
Unsecured Network	Network
Unused Ports Enable	Network
Weak/lack Encryption in Communication	Network
Physical properties of the power system	Network
Wifi De-authentication	Network
Insecure traffic control	Network
Centralized architecture	Network
Access Malicious Link	Peopleware
Identifying the Product Vendor	Peopleware
Knowledge the System	Peopleware
Lack of Technical Support	Peopleware
Personal and Social Circumstances	Peopleware
Phishing	Peopleware
Social Engineering	Peopleware
Untrusted Device Acquisition	Peopleware
Vendor Security Posture	Peopleware