CWE-IoT / IoT Category Weakness Type	Routers	IP Cameras	Printers	Medical devices	IoT Actuators	IoT Sensors	Smart Wearable Devices	IoT Application Layer Protocols
CWE- 20-improper input validation	CVE-2017-17215, CVE-2017-9675, CVE-2017-18867	CVE-2018-9158	CVE-2013-4615	CVE-2017-12701, CVE-2017-7730	CVE-2019-17210, CVE-2018-16528	CVE-2018-14889, CVE-2014-2360, CVE-2018-11315		CVE-2018-8030, CVE-2018-1298, CVE-2017-11408, CVE-2016-4974, CVE-2016-2173, CVE-2018-15323, CVE-2014-0923, CVE-2014-0922, CVE-2015-7559, CVE-2017-15699, CVE-2019-1845, CVE-2017-5602, CVE-2017-5603, CVE-2017-5604, CVE-2017-5605
CWE-287-Improper Authentication	CVE-2018-9032, CVE-2017-14698	CVE-2013-6117	CVE-2018-11692, CVE-2017-7588	CVE-2017-14002(ICS-CERT) , CVE-2017-14006(ICS-CERT), CVE-2017-14008(ICS-CERT),CVE-2019-10964, CVE-2018-14786,CVE-2020-27269, CVE-2017-12721, CVE-2020-15486, CVE-2020-28973, CVE-2017-7728,CVE-2020-27266	CVE-2018-19616	CVE-2021-20107		CVE-2016-4432, CVE-2012-4446, CVE-2012-3467,CVE-2017-7650, CVE-2014-6116
CWE-200- Exposure of Sensitive Information to an Unauthorized Actor	CVE-2018-10106, CVE-2017-5892, CVE-2014-8361,	CVE-2017-7923, CVE-2018-11653, CVE-2018-11654, CVE-2015-2884	CVE-2018-16710, CVE-2020-27290	CVE-2017-11578		CVE-2016-2311(NIST), CVE-2016-0864		CVE-2017-9868
CWE-119-Improper Restriction of Operations within the Bounds of a Memory Buffer						CVE-2017-18303, CVE-2012-3901	CVE-2017-17773	CVE-2018-17614, CVE-2016-10523, CVE-2018-19417
CWE-79- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		CVE-2014-9517,	CVE-2018-11581 ,,CVE-2018-5550, CVE-2018-14899		CVE-2018-16210	CVE-2016-0866		CVE-2015-0862, CVE-2017-7296, CVE-2017-4965
CWE-798- Use of Hard-coded Credentials	CVE-2021-27149			CVE-2017-14002(NIST), CVE-2017-14006(NIST), CVE-2017-14008(NIST),CVE-2020-27278, CVE-2020-27256, CVE-2020-12039, CVE-2017-12726, CVE-2017-12725, CVE-2017-12724,CVE-2018-14801, CVE-2018-8870		CVE-2021-27952		CVE-2018-15720
CWE-125- Out-of-bounds Read				CVE-2017-12722, CVE-2021-27408	CVE-2019-13120			
CWE-787-Out-of-bounds Write	CVE-2018-1156				CVE-2020-9395	CVE-2020-8997, CVE-2021-27954		CVE-2018-853, CVE-2019-17212, CVE-2018-5879, CVE-2018-11993, CVE-2017-2894
CWE-319-Cleartext Transmission of Sensitive Information				CVE-2020-15482, CVE-2019-9860, CVE-2018-11399		CVE-2018-11399		CVE-2018-11050, CVE-2019-15135
CWE-310-Cryptographic Issue				CVE-2019-14261, CVE-2019-9861		CVE-2014-2379,		CVE-2015-1500
CWE-306- Missing Authentication for Critical Function	CVE-2020-15834			CVE-2020-27376		CVE-2020-3448		
CWE-312-Cleartext Storage of Sensitive Information								CVE-2018-8030, CVE-2018-1298, CVE-2017-11408, CVE-2016-4974, CVE-2016-2173, CVE-2018-15323, CVE-2014-0923, CVE-2014-0922, CVE-2015-7559, CVE-2017-15699, CVE-2019-1845, CVE-2017-5605
CWE-264-Permissions, Privileges, and Access Controls rs	CVE-2014-9583,		CVE-2012-4964			CVE-2013-4860	CVE-2013-4872	CVE-2015-1499

CWE-IoT / IoT Category Weakness Type	Routers	IP Cameras	Printers	Medical devices	IoT Actuators	IoT Sensors	Smart Wearable Devices	IoT Application Layer Protocols
CWE-78- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	CVE-2017-16957, CVE-2019-16920, CVE-2019-8319	CVE-2018-10660		CVE-2020-27373				
CWE-120-Classic Buffer Overflow				CVE-2022-22819	CVE-2019-17518			
CWE-284-Improper Access Control				CVE-2020-10627				CVE-2016-4432, CVE-2012-4446, CVE-2012-3467,CVE-2017-7650, CVE-2014-6118
CWE-312-Cleartext Storage of Sensitive Information								CVE-2018-8030, CVE-2018-1298, CVE-2017-11408, CVE-2016-4974, CVE-2016-2173, CVE-2018-15323, CVE-2014-0923, CVE-2014-0922, CVE-2015-7559, CVE-2017-15699, CVE-2019-1845, CVE-2017-5605
CWE-255-Credentials Management Errors						CVE-2016-2311(NIST), CVE-2016-0865		CVE-2016-1307
CWE-309-Missing Encryption of Sensitive Data				CVE-2020-15483				CVE-2018-853, CVE-2019-17212, CVE-2018-5879, CVE-2018-11994
CWE-770-Allocation of Resources Without Limits or Throttling								CVE-2015-0862, CVE-2017-7296, CVE-2017-4966
CWE-311- Missing Encryption of Sensitive Data				CVE-2018-10825, CVE-2019-9862, CVE-2018-8864, CVE-2017-7729	CVE-2018-20100			
CWE-327-Use of a Broken or Risky Cryptographic Algorithm						CVE-2020-7339, CVE-2018-6402		CVE-2018-19418
CWE-290-Authentication By pass by Spoofing				CVE-2020-27276				CVE-2016-4432, CVE-2012-4446, CVE-2012-3467,CVE-2017-7650, CVE-2014-6119
CWE-707-Improper Neutralization								CVE-2018-853, CVE-2019-17212, CVE-2018-5879, CVE-2018-11995
CWE-862-Missing Authorization				CVE-2020-13425				
CWE-285- Improper Authorization								CVE-2015-1502

CWE-IoT / IoT Category Weakness Type	Routers	IP Cameras	Printers	Medical devices	IoT Actuators	IoT Sensors	Smart Wearable Devices	IoT Application Layer Protocols
CWE-352-Cross-Site Request Forgery (CSRF)	CVE-2017-5891,					CVE-2016-0863		
CWE-434-Unrestricted Upload of File with Dangerous Type								CVE-2017-15701, CVE-2017-7651, CVE-2019-9751
CWE-94-Improper Control of Generation of Code ('Code Injection')						CVE-2014-2378		
CWE-326-Inadequate Encryption Strength					CVE-2017-14797			CVE-2017-9870
CWE-191-Integer Underflow (Wrap or Wraparound)								CVE-2017-15701, CVE-2017-7651, CVE-2019-9752
CWE-309-Missing Encryption of Sensitive Data				CVE-2020-15483				CVE-2018-853, CVE-2019-17212, CVE-2018-5879, CVE-2018-11994
CWE-294-Authentication By Pass				CVE-2020-27374, CVE-2021-40170,CVE-2019-9659				
CWE-88-Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')								CVE-2015-0862, CVE-2017-7296, CVE-2017-4967
CWE-347-Improper Verification of Cryptographic Signature								CVE-2018-11050, CVE-2019-15137
CWE-427- Uncontrolled Search Path Element								CVE-2017-9871
CWE-362-Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')								CVE-2018-15721
CWE-345- Insufficient Verification of Data Authenticity								
CWE-668-Exposure of Resource to Wrong Sphere				CVE-2018-18068				

CWE-IoT / IoT Category / Weakness Type	Routers	IP Cameras	Printers	Medical devices	IoT Actuators	IoT Sensors	Smart Wearable Devices	IoT Application Layer Protocols
CWE-693-Protection Mechanism Failure								CVE-2015-1501
CWE-327-Use of a Broken or Risky Cryptographic Algorithm								
CWE-295-Improper Certificate validation				CVE-2017-7726				
CWE-399-Resource Management Errors	CVE-2012-4621					CVE-2019-1957		CVE-2017-9869
CWE-89-Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')								CVE-2016-4432, CVE-2012-4446, CVE-2012-3467,CVE-2017-7650, CVE-2014-6117
CWE-400-Uncontrolled Resource Consumption	CVE-2018-10070							CVE-2017-15701, CVE-2017-7651, CVE-2019-9750
CWE-22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	CVE-2018-14847, CVE-2015-7254							
CWE-113-Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')								CVE-2018-19419
CWE-682- Incorrect Calculation								CVE-2018-11050, CVE-2019-15136
CWE-922-Insecure Storage of Sensitive Information		CVE-2017-7253,						
CWE-330-Use of Insufficiently Random Values				CVE-2019-9863,CVE-2020-27264	CVE-2017-6026			
CWE- 22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		CVE-2014-9234						
CWE-388-Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)						CVE-2014-2362		

CWE-IoT / IoT Category Weakness Type	Routers	IP Cameras	Printers	Medical devices	IoT Actuators	IoT Sensors	Smart Wearable Devices	IoT Application Layer Protocols
CWE-77-Improper Neutralization of Special Elements used in a Command ('Command Injection')								
CWE-1263-Improper Physical Access Controln				CVE-2021-40171				
CWE-522-Insufficiently Protected Credentials								
CWE-340-Key Management Errors						CVE-2014-2361		
CWE-88-Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')								CVE-2015-0862, CVE-2017-7296, CVE-2017-4967
CWE-77-Improper Neutralization of Special Elements used in a Command ('Command Injection')								
CWE-294-Authentication By Pass				CVE-2020-27374, CVE-2021-40170,CVE-2019-9659				
CWE-862-Missing Authorization				CVE-2020-13425				
CWE-1263-Improper Physical Access Control				CVE-2021-40171				
CWE-347-Improper Verification of Cryptographic Signature								CVE-2018-11050, CVE-2019-15137
CWE-120-Classic Buffer Overflow				CVE-2022-22819	CVE-2019-17518			
CWE-668-Exposure of Resource to Wrong Sphere				CVE-2018-18068				
CWE-918-Server-Side Request Forgery (SSRF)								

CWE-IoT / IoT Category Weakness Type	Routers	IP Cameras	Printers	Medical devices	IoT Actuators	IoT Sensors	Smart Wearable Devices	IoT Application Layer Protocols
CWE-312-Cleartext Storage of Sensitive Information								
CWE-78-Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	CVE-2019-16920,CVE-2019-8319							
CWE-522-Insufficiently Protected Credentials								
CWE-290-Authentication By pass by Spoofing				CVE-2020-27276				CVE-2016-4432, CVE-2012-4446, CVE-2012-3467,CVE-2017-7650, CVE-2014-6119
CWE-427- Uncontrolled Search Path Element								CVE-2017-9871
CWE-285- Improper Authorization								CVE-2015-1502
CWE-345- Insufficient Verification of Data Authenticity								
CWE-No-info								CVE-2018-15722

CWE-IoT / IoT Category / Weakness Type	IoT Wireless Communication Protocols (BLE, ZigBee, Z-wave, Wi-Fi, etc…)	Smart Phones	IoT Gateway	IoT Technologies (RFID, QR codes, NFC, etc.)	Smart Vehicles	Smart Hub Controllers
CWE- 20-improper input validation	CVE-2015-8732, CVE-2015-6244, CVE-2019-19192,CVE-2019-19193	CVE-2016-4038, CVE-2014-9866, CVE-2017-15322	CVE-2020-4207	CVE-2019-19195, CVE-2018-4833, CVE-2015-6839, CVE-2014-0239		
CWE-287-Improper Authentication	CVE-2019-19194			CVE-2020-15802,CVE-2020-25183		CVE-2017-16348
CWE-200- Exposure of Sensitive Information to an Unauthorized Actor		CVE-2017-15814, CVE-2017-0709, CVE-2016-2813, CVE-2018-7930, CVE-2016-3761, CVE-2015-4033, CVE-2016-1562	CVE-2018-18390	CVE-2017-18642, CVE-2017-17280		CVE-2017-14443, CVE-2018-15125, CVE-2016-2311
CWE-119-Improper Restriction of Operations within the Bounds of a Memory Buffer		CVE-2016-3934,CVE-2014-9786, CVE-2017-17225		CVE-2013-0656, CVE-2018-3900, CVE-2018-3899, CVE-2018-3898	CVE-2017-9647, CVE-2017-9633, CVE-2017-17773	CVE-2017-16347, CVE-2017-16346, CVE-2017-16345, CVE-2017-16344, CVE-2017-16343, CVE-2017-16342, CVE-2017-16341, CVE-2017-16340, CVE-2017-16339, CVE-2017-16338, CVE-2017-16337, CVE-2017-16252, CVE-2017-14455, CVE-2017-14453, CVE-2017-14452, CVE-2017-14447, CVE-2017-14446, CVE-2017-14445, CVE-2017-14444, CVE-2018-3925, CVE-2018-3917, CVE-2018-3912,CVE-2018-3903, CVE-2018-3905, CVE-2018-3904, CVE-2018-3902, CVE-2018-3897, CVE-2018-3896, CVE-2018-3895, CVE-2018-3894, CVE-2018-3893, CVE-2018-3878, CVE-2018-3877, CVE-2018-3876, CVE-2018-3874, CVE-2018-3873, CVE-2018-3872, CVE-2018-3866, CVE-2018-3865, CVE-2018-3864, CVE-2018-3863
CWE-79-Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')			CVE-2020-6804,CVE-2022-23136,CVE-2021-40517,CVE-2020-10633,CVE-2018-16199	CVE-2018-5303, CVE-2014-8672		
CWE-798- Use of Hard-coded Credentials			CVE-2021-40422,CVE-2021-40519,CVE-2019-17667,CVE-2019-17663,CVE-2017-2236,CVE-2018-16201, CVE-2021-33220, CVE-2021-33219, CVE-2021-33218			
CWE-125- Out-of-bounds Read						
CWE-787-Out-of-bounds Write	CVE-2020-27301, CVE-2020-27302		CVE-2021-33217			CVE-2018-6692, CVE-2018-3919, CVE-2018-3916, CVE-2018-3915, CVE-2018-3914, CVE-2018-3913, CVE-2018-3906, CVE-2018-3880, CVE-2018-3867, CVE-2018-8531
CWE-319-Cleartext Transmission of Sensitive Information				CVE-2020-11539, CVE-2020-14157	CVE-2018-18071	
CWE-310-Cryptographic Issue						CVE-2013-6952, CVE-2013-6951, CVE-2013-6950, CVE-2015-4080
CWE-306-Missing Authentication for Critical Function			CVE-2021-33221	CVE-2021-20107		
CWE-312-Cleartext Storage of Sensitive Information			CVE-2018-18394			
CWE-264-Permissions, Privileges, and Access Controls		CVE-2016-3903, CVE-2016-3798,CVE-2014-9890, CVE-2014-9868, CVE-2014-9783,CVE-2014-9782				CVE-2013-6949

CWE-IoT / IoT Category / Weakness Type	IoT Wireless Communication Protocols (BLE, ZigBee, Z-wave, Wi-Fi, etc…)	Smart Phones	IoT Gateway	IoT Technologies (RFID, QR codes, NFC, etc.)	Smart Vehicles	Smart Hub Controllers
CWE-78- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')			CVE-2019-12787, CVE-2019-13128, CVE-2020-24552, CVE-2018-16200, CVE-2017-2237	CVE-2020-27542		
CWE-120-Classic Buffer Overflow	CVE-2019-19196	CVE-2017-0481				
CWE-284-Improper Access Control	CVE-2016-5058, CVE-2016-5054				CVE-2016-2354	CVE-2019-11895
CWE-312-Cleartext Storage of Sensitive Information			CVE-2018-18394			
CWE-255-Credentials Management Errors						
CWE-309-Missing Encryption of Sensitive Data				CVE-2019-11523		
CWE-770-Allocation of Resources Without Limits or Throttling			CVE-2019-9012	CVE-2017-7696		
CWE-311- Missing Encryption of Sensitive Data	CVE-2020-9058, CVE-2020-9057		CVE-2021-37189			CVE-2017-5251
CWE-327-Use of a Broken or Risky Cryptographic Algorithm						
CWE-290-Authentication By pass by Spoofing				CVE-2020-10135		
CWE-707-Improper Neutralization						CVE-2018-3918
CWE-862-Missing Authorization			CVE-2020-27220,CVE-2018-13109			
CWE-285- Improper Authorization	CVE-2020-9061					
CWE-352-Cross-Site Request Forgery (CSRF)			CVE-2021-40518,CVE-2017-2238			
CWE-434-Unrestricted Upload of File with Dangerous Type				CVE-2021-32089		CVE-2018-3832,

CWE-IoT / IoT Category Weakness Type	IoT Wireless Communication Protocols (BLE, ZigBee, Z-wave, Wi-Fi, etc…)	Smart Phones	IoT Gateway	IoT Technologies (RFID, QR codes, NFC, etc.)	Smart Vehicles	Smart Hub Controllers
CWE-94-Improper Control of Generation of Code ('Code Injection')						CVE-2013-6948
CWE-326-Inadequate Encryption Strength			CVE-2021-37188			CVE-2018-15124
CWE-191-Integer Underflow (Wrap or Wraparound)	CVE-2018-3926					
CWE-309-Missing Encryption of Sensitive Data				CVE-2019-11523		
CWE-294-Authentication By Pass						
CWE-88-Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')						CVE-2018-3856
CWE-347-Improper Verification of Cryptographic Signature						
CWE-427- Uncontrolled Search Path Element				CVE-2017-2286, CVE-2017-2287		
CWE-362-Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')						
CWE-345- Insufficient Verification of Data Authenticity	CVE-2020-10137					
CWE-668-Exposure of Resource to Wrong Sphere			CVE-2021-20999			
CWE-693-Protection Mechanism Failure					CVE-2018-9322, CVE-2018-9320, CVE-2018-9318, CVE-2018-9314, CVE-2018-9313, CVE-2018-9312, CVE-2018-9311	
CWE-327-Use of a Broken or Risky Cryptographic Algorithm					CVE-2018-16806, CVE-2017-14937	
CWE-295-Improper Certificate validation						CVE-2018-3927

CWE-IoT / IoT Category / Weakness Type	IoT Wireless Communication Protocols (BLE, ZigBee, Z-wave, Wi-Fi, etc…)	Smart Phones	IoT Gateway	IoT Technologies (RFID, QR codes, NFC, etc.)	Smart Vehicles	Smart Hub Controllers
CWE-399-Resource Management Errors						
CWE-89-Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')						CVE-2018-3879
CWE-400-Uncontrolled Resource Consumption	CVE-2020-9060, CVE-2020-9059			CVE-2014-3651		
CWE-22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')			CVE-2019-11603,CVE-2019-11601, CVE-2022-23135, 2021-27328,CVE-2018-7933, CVE-2021-33215			
CWE-113-Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')						CVE-2018-3911
CWE-682- Incorrect Calculation						
CWE-922-Insecure Storage of Sensitive Information		CVE-2017-5249				
CWE-330-Use of Insufficiently Random Values						
CWE- 22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')						
CWE-388-Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)						
CWE-77-Improper Neutralization of Special Elements used in a Command ('Command Injection'))					CVE-2016-9337	
CWE-1263-Improper Physical Access Control						
CWE-522-Insufficiently Protected Credentials			CVE-2021-40520			
CWE-340-Key Management Errors						

CWE-IoT / IoT Category Weakness Type	IoT Wireless Communication Protocols (BLE, ZigBee, Z-wave, Wi-Fi, etc…)	Smart Phones	IoT Gateway	IoT Technologies (RFID, QR codes, NFC, etc.)	Smart Vehicles	Smart Hub Controllers
CWE-88-Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')						CVE-2018-3856
CWE-77-Improper Neutralization of Special Elements used in a Command ('Command Injection')					CVE-2016-9337	
CWE-294-Authentication By Pass						
CWE-862-Missing Authorization			CVE-2020-27220,CVE-2018-13109			
CWE-1263-Improper Physical Access Control						
CWE-347-Improper Verification of Cryptographic Signature						
CWE-120-Classic Buffer Overflow	CVE-2019-19196	CVE-2017-0481				
CWE-668-Exposure of Resource to Wrong Sphere			CVE-2021-20999			
CWE-918-Server-Side Request Forgery (SSRF)			CVE-2019-11897			
CWE-312-Cleartext Storage of Sensitive Information			CVE-2018-18394			
CWE-78-Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')			CVE-2019-13128,CVE-2020-24552, CVE-2018-16200,CVE-2017-2237			
CWE-522-Insufficiently Protected Credentials			CVE-2021-40520			
CWE-290-Authentication By pass by Spoofing				CVE-2020-10135		

CWE-IoT / IoT Category Weakness Type	IoT Wireless Communication Protocols (BLE, ZigBee, Z-wave, Wi-Fi, etc…)	Smart Phones	IoT Gateway	IoT Technologies (RFID, QR codes, NFC, etc.)	Smart Vehicles	Smart Hub Controllers
CWE-427- Uncontrolled Search Path Element				CVE-2017-2286, CVE-2017-2287		
CWE-285- Improper Authorization	CVE-2020-9061					
CWE-345- Insufficient Verification of Data Authenticity	CVE-2020-10137					
CWE-No-info					CVE-2015-5611	