CVE-IoT / IoT Component	IoT Gateway	Pressure Adjusting Machine	Low-range wireless communication Technologies	Medical Ventilator	Sensors	Infusion Pump
CVE-2017-7730	CAPEC-482: TCP Flood, CAPEC-469: HTTP DoS					
CVE-2020-4207	CAPEC-8: Buffer Overflow through API calls					
CVE-2017-14447	CAPEC-115: Authentication bypass, CAPEC-8: Buffer Overflow through API calls					
CVE-2017-16252	CAPEC-115: Authentication bypass, CAPEC-8: Buffer Overflow through API calls					
CVE-2017-14455	CAPEC-8: Buffer Overflow through API calls,					
CVE-2021-33217	CAPEC-8: Buffer Overflow through API calls, CAPEC-115: Authentication bypass					
CVE-2017-5251	CAPEC-157: Sniffing Attacks, CAPEC-94: Adversary in the Middle (AITM)					
CVE-2017-14443	CAPEC-131: Resource Leak Exposure					
CVE-2017-14443	CAPEC-37: Retrieve Embedded Sensitive Data					
CVE-2018-15125	CAPEC-37: Retrieve Embedded Sensitive Data, CAPEC-653: Use of Known Operating System Credentials					
CVE-2018-16201	CAPEC-37: Retrieve Embedded Sensitive Data, CAPEC-88: OS Command Injection, CAPEC-653: Use of Known Operating System Credentials					
CVE-2021-33218	CAPEC-37: Retrieve Embedded Sensitive Data,					
CVE-2021-33219	CAPEC-37: Retrieve Embedded Sensitive Data,					
CVE-2018-18394	CAPEC-37: Retrieve Embedded Sensitive Data,					
CVE-2021-27328	CAPEC-37: Retrieve Embedded Sensitive Data, CAPEC-115: Authentication bypass, CAPEC-126: Path Traversal					
CVE-2013-6948	CAPEC-201: Serialized Data External Links,					
CVE-2017-7728	CAPEC-115: Authentication bypass, CAPEC-248: Command Injection, CAPEC-475: Signature Spoofing by Improper Validation					
CVE-2017-16348	CAPEC-115: Authentication bypass, CAPEC-486: UDP Flood					
CVE-2021-40422	CAPEC-115: Authentication bypass, CAPEC-273: HTTP Response Smuggling					
CVE-2020-3448	CAPEC-115: Authentication bypass,					
CVE-2021-37188	CAPEC-115: Authentication bypass, CAPEC-638: Altered Component Firmware					
CVE-2019-13128	CAPEC-114: Authentication abuse, CAPEC-88: OS Command Injection					
CVE-2018-16200	CAPEC-114: Authentication abuse,					
CVE-2017-2237	CAPEC-114: Authentication abuse,					
CVE-2019-12787	CAPEC-250: XML Injection					
CVE-2020-24552	CAPEC-242: Code Injection,					
CVE-2017-7729	CAPEC-102: Session Sidejacking, CAPEC-114: Authentication abuse					
CVE-2021-37189	CAPEC-102: Session Sidejacking					
CVE-2016-0864	CAPEC-560: Use of Known Domain Credentials					
CVE-2016-0866	Cross-site scripting (XSS)					
CVE-2016-0863	CAPEC-62: Cross Site Request Forgery, CAPEC-593: Session Hijacking					
CVE-2019-11897	CAPEC-62: Cross Site Request Forgery					
CVE-2021-33215	CAPEC-126: Path Traversal					
CVE-2022-23135	CAPEC-126: Path Traversal					
CVE-2021-40520	CAPEC-600: Credential Stuffing					
CVE-2017-12701		CAPEC-125: Flooding Attacks				
CVE-2020-9061			CAPEC-125: Flooding Attacks			
CVE-2020-9060			CAPEC-125: Flooding Attacks			
CVE-2020-9059			CAPEC-125: Flooding Attacks			
CVE-2019-19192			CAPEC-100: Overflow Buffer, CAPEC-25: Forced Deadlock			
CVE-2019-19193			CAPEC-100: Overflow Buffer			
CVE-2019-19195			CAPEC-100: Overflow Buffer			
CVE-2019-19196			CAPEC-100: Overflow Buffer, CAPEC-114: Authentication abuse			
CVE-2020-27301			CAPEC-100: Overflow Buffer			
CVE-2020-27302			CAPEC-100: Overflow Buffer			
CVE-2020-10135			CAPEC-114: Authentication abuse			
CVE-2019-19194			CAPEC-114: Authentication abuse			
CVE-2020-10137			CAPEC-114: Authentication abuse, CAPEC-651: Eavesdropping			
CVE-2020-15802			CAPEC-94: Adversary in the Middle (AiTM), CAPEC-668: Key Negotiation of Bluetooth Attack (KNOB)			
CVE-2016-5058			CAPEC-94: Adversary in the Middle (AiTM)			
CVE-2016-5054			CAPEC-94: Adversary in the Middle (AiTM)			
CVE-2020-9057			CAPEC-94: Adversary in the Middle (AiTM), CAPEC-651: Eavesdropping			
CVE-2020-9058			CAPEC-94: Adversary in the Middle (AiTM), CAPEC-651: Eavesdropping			
CVE-2018-3926			CAPEC-273: HTTP Response Smuggling			
CVE-2015-8732			CAPEC-540: Overread Buffers			
CVE-2015-6244			CAPEC-540: Overread Buffers			

CVE-2020-27290				CAPEC-507: Physical Theft, CAPEC-95: Lab-Injection-Tampering-Fueling	CAPEC-115: Authentication bypass	
CVE-2020-27278				CAPEC-507: Physical Theft		
CVE-2014-2360					CAPEC-100: Overflow Buffer	
CVE-2021-27954					CAPEC-100: Overflow Buffer	
CVE-2018-8870					CAPEC-507: Physical Theft	
CVE-2014-2361					CAPEC-115: Authentication bypass, CAPEC-507: Physical Theft	
CVE-2017-11578					CAPEC-157: Sniffing Attacks	
CVE-2020-15406					CAPEC-152: Sniffing Attacks, CAPEC-94: Adversary in the Middle (AITM)	
CVE-2020-11539					CAPEC-152: Sniffing Attacks, CAPEC-94: Adversary in the Middle (AITM)	
CVE-2019-18252					CAPEC-37: Retrieve Embedded Sensitive Data	
CVE-2018-10825					CAPEC-115: Authentication bypass, CAPEC-148: Content Spoofing	
CVE-2021-20107					CAPEC-629: Exploitation of Improperly Configured or Implemented Memory Protections, CAPEC-115: Authentication bypass	
CVE-2013-4860					CAPEC-115: Authentication bypass	
CVE-2019-13916					CAPEC-100: Overflow Buffers, CAPEC-153: Input Data Manipulation	
CVE-2020-25183					CAPEC-114, CAPEC-151, CAPEC-148	
CVE-2020-11957					CAPEC-152: Sniffing Attacks, CAPEC-94: Adversary in the Middle (AITM), CAPEC-112: Brute Force, CAPEC-665: Bluetooth Impersonation Attacks (BIAS), CAPEC-102: Session Sidejacking	
CVE-2019-16336					CAPEC-158, CAPEC-130, CAPEC-152, CAPEC-231, CAPEC-100, CAPEC-26	
CVE-2019-17520					CAPEC-152, CAPEC-157	
CVE-2019-17061					CAPEC-157, CAPEC-100, CAPEC-25, CAPEC-153	
CVE-2019-17519					CAPEC-157, CAPEC-100, CAPEC-231, CAPEC-153	
CVE-2019-17060					CAPEC-157, CAPEC-100, CAPEC-25, CAPEC-153	
CVE-2019-17517					CAPEC-100, CAPEC-152, CAPEC-157	
CVE-2019-17518					CAPEC-100, CAPEC-231, CAPEC-157, CAPEC-153	
CVE-2020-15531					CAPEC-157, CAPEC-100, CAPEC-152, CAPEC-248	
CVE-2020-15532					CAPEC-157, CAPEC-100, CAPEC-152, CAPEC-248	
CVE-2019-15948					CAPEC-157, CAPEC-100, CAPEC-152, CAPEC-248	
CVE-2020-13594					CAPEC-157, CAPEC-152	
CVE-2022-45192					CAPEC-157, CAPEC-152	
CVE-2022-45191					CAPEC-157, CAPEC-152	
CVE-2020-13595					CAPEC-157, CAPEC-152	
CVE-2020-13593					CAPEC-157, CAPEC-152	
CVE-2020-11114					CAPEC-157, CAPEC-100, CAPEC-152, CAPEC-248	
CVE-2022-45190					CAPEC-94, CAPEC-667, CAPEC-115	
CVE-2023-27917	CAPEC-88, CAPEC-114					
CVE-2020-24552	CAPEC-88, CAPEC-153					
CVE-2019-13128	CAPEC-88, CAPEC-114					
CVE-2022-29556	CAPEC-664					
CVE-2020-3702	CAPEC-115, CAPEC-37, CAPEC-117					
CVE-2021-20999	CAPEC-300, CAPEC-115, CAPEC-118, CAPEC-157					
CVE-2021-22547	CAPEC-100, CAPEC-248, CAPEC-37, CAPEC-153					
CVE-2017-7728	CAPEC-115, CAPEC-248					
CVE-2017-16348	CAPEC-114, CAPEC-248, CAPEC-153					
CVE-2018-15125	CAPEC-37					
CVE-2017-16348	CAPEC-114, CAPEC-248, CAPEC-153					
CVE-2017-7728	CAPEC-115, CAPEC-248					
CVE-2021-22547	CAPEC-100, CAPEC-248, CAPEC-37, CAPEC-153					
CVE-2021-20999	CAPEC-300, CAPEC-115, CAPEC-118, CAPEC-157					
CVE-2020-3702	CAPEC-115, CAPEC-37, CAPEC-117					
CVE-2022-29556	CAPEC-664					
CVE-2019-13128	CAPEC-88, CAPEC-114					
CVE-2020-24552	CAPEC-88, CAPEC-153					
CVE-2023-27917	CAPEC-88, CAPEC-114					
CVE-2022-45190					CAPEC-94, CAPEC-667, CAPEC-115	
CVE-2020-11114					CAPEC-157, CAPEC-100, CAPEC-152, CAPEC-248	
CVE-2020-13593					CAPEC-157, CAPEC-152	
CVE-2020-13595					CAPEC-157, CAPEC-152	
CVE-2022-45191					CAPEC-157, CAPEC-152	
CVE-2022-45192					CAPEC-157, CAPEC-152	
CVE-2020-13594					CAPEC-157, CAPEC-152	
CVE-2019-15948					CAPEC-157, CAPEC-100, CAPEC-152, CAPEC-248	
CVE-2020-15532					CAPEC-157, CAPEC-100, CAPEC-152, CAPEC-248	
CVE-2020-15531					CAPEC-157, CAPEC-100, CAPEC-152, CAPEC-248	
CVE-2019-17518					CAPEC-100, CAPEC-231, CAPEC-157, CAPEC-153	
CVE-2019-17517					CAPEC-100, CAPEC-152, CAPEC-157	
CVE-2019-17060					CAPEC-157, CAPEC-100, CAPEC-25, CAPEC-153	
CVE-2019-17519					CAPEC-157, CAPEC-100, CAPEC-231, CAPEC-153	
CVE-2019-17061					CAPEC-157, CAPEC-100, CAPEC-25, CAPEC-153	
CVE-2019-17520					CAPEC-152, CAPEC-157	
CVE-2019-16336					CAPEC-158, CAPEC-130, CAPEC-152, CAPEC-231, CAPEC-100, CAPEC-26	
CVE-2020-11957					CAPEC-157: Sniffing Attacks, CAPEC-94: Adversary in the Middle (AITM), CAPEC-112: Brute Force, CAPEC-665: Bluetooth Impersonation Attacks (BIAS), CAPEC-102: Session Sidejacking	
CVE-2018-6402					CAPEC-114: Authentication Abuse, CAPEC-615: EAP Twin WiFi Attack	
CVE-2018-11315					CAPEC-114: Authentication Abuse, CAPEC-275: DNS Rebinding	
CVE-2013-4860					CAPEC-115: Authentication bypass	
CVE-2018-11399					CAPEC-117: Interception	
CVE-2020-27373					CAPEC-88: OS Command Injection	
CVE-2019-18246					CAPEC-114: Authentication Abuse	
CVE-2018-6402					CAPEC-114: Authentication Abuse, CAPEC-615: EAP Twin WiFi Attack	
CVE-2018-11315					CAPEC-114: Authentication Abuse, CAPEC-275: DNS Rebinding	
CVE-2020-18183					CAPEC-114, CAPEC-151, CAPEC-148	
CVE-2019-13916					CAPEC-100: Overflow Buffers, CAPEC-153: Input Data Manipulation	
CVE-2020-10061					CAPEC-100: Overflow Buffers, CAPEC-130: Excessive Allocation, CAPEC-153: Input Data Manipulation	
CVE-2023-28116					CAPEC-100: Overflow Buffers	
CVE-2014-2362					CAPEC-97: Cryptanalysis	
CVE-2014-2378					CAPEC-686: Install Malicious Extension	
CVE-2021-27952					CAPEC-560: Use of Known Domain Credentials	
CVE-2020-8997					CAPEC-629: Exploitation of Improperly Configured or Implemented Memory Protections	
CVE-2016-2311					CAPEC-633: Use of Known Operating System Credentials	
CVE-2014-2379					CAPEC-102: Session Sidejacking	
CVE-2018-11399					CAPEC-117: Interception	
CVE-2020-27373					CAPEC-88: OS Command Injection	
CVE-2019-18246					CAPEC-114: Authentication Abuse	
CVE-2020-27278					CAPEC-507: Physical Theft	
CVE-2014-2360					CAPEC-100: Overflow Buffer	
CVE-2021-27954					CAPEC-100: Overflow Buffer	
CVE-2018-8870					CAPEC-507: Physical Theft	
CVE-2014-2361					CAPEC-115: Authentication bypass, CAPEC-507: Physical Theft	
CVE-2017-11578					CAPEC-157: Sniffing Attacks	
CVE-2020-15406					CAPEC-152: Sniffing Attacks, CAPEC-94: Adversary in the Middle (AITM)	
CVE-2020-11539					CAPEC-152: Sniffing Attacks, CAPEC-94: Adversary in the Middle (AITM)	
CVE-2019-18252					CAPEC-37: Retrieve Embedded Sensitive Data	
CVE-2018-10825					CAPEC-115: Authentication bypass, CAPEC-148: Content Spoofing	
CVE-2021-20107					CAPEC-629: Exploitation of Improperly Configured or Implemented Memory Protections, CAPEC-115: Authentication bypass	
CVE-2013-4860					CAPEC-115: Authentication bypass	