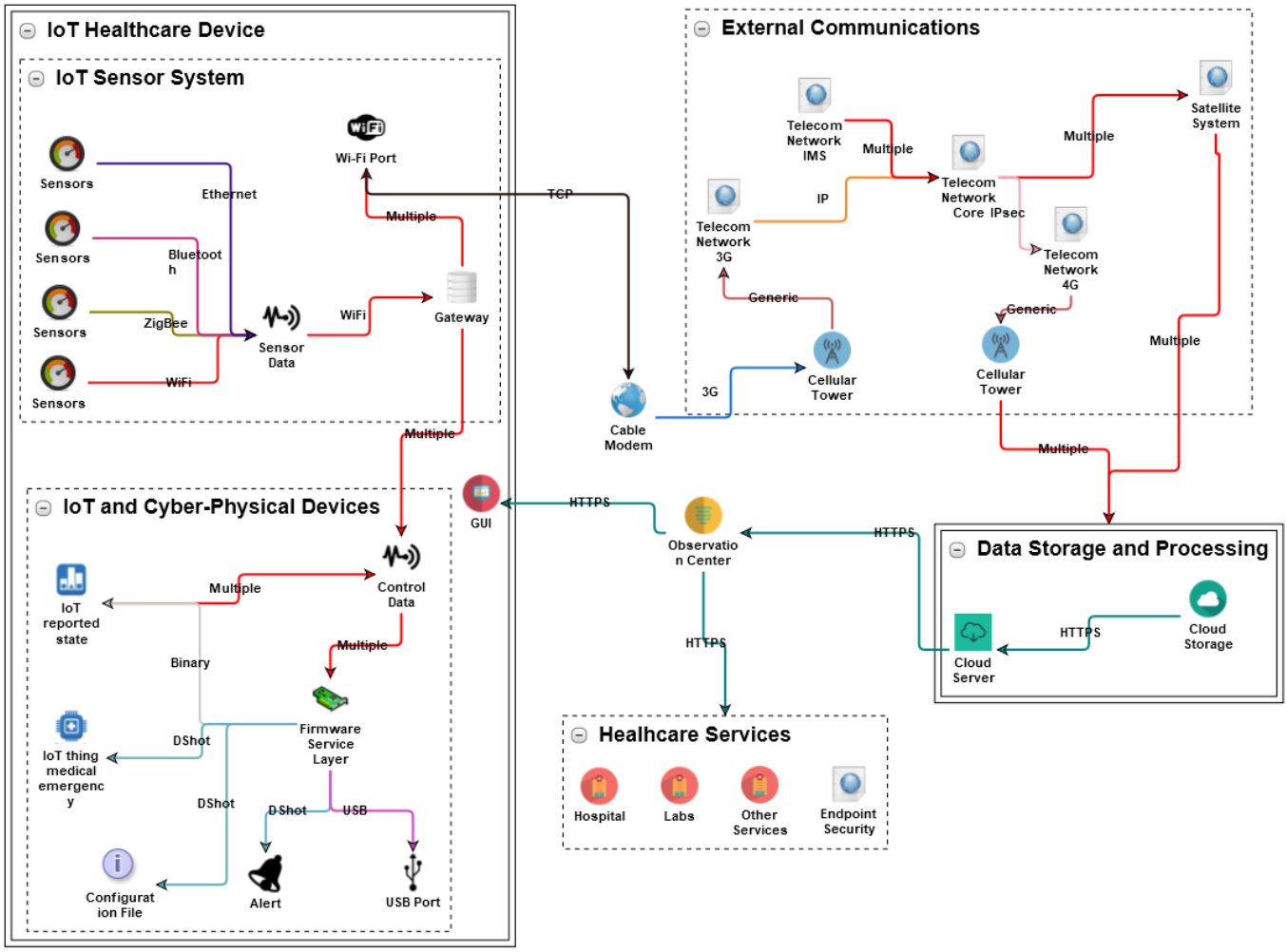
ThreatModeler
Identify • Classify • Prioritize • Mitigate

Healthcare Cyber Physical System - 2

03/22/2018

Threat Model



Description

Threats

Threat	Source	Risk	Status	Date Created
Sensitive Data Exposure	Sensor Data	Very High	Open	03/22/2018
Sensitive Data Exposure	Other Services	Very High	Open	03/22/2018
Man in the Middle Attack	Wi-Fi Port	Very High	Open	03/22/2018

Wi-Fi Jamming	Wi-Fi Port	High	Open	03/22/2018
WiFi MAC Address Tracking	Wi-Fi Port	Very High	Open	03/22/2018
WiFi SSID Tracking	Wi-Fi Port	Very High	Open	03/22/2018
Malicious Software Download	Firmware Service Layer	Very High	Open	03/22/2018
Sensitive Data Exposure	Control Data	Very High	Open	03/22/2018
Sensitive Data Exposure	Labs	Very High	Open	03/22/2018
Man in the Middle Attack	Gateway	Very High	Open	03/22/2018
Sensitive Data Exposure	Cloud Storage	Very High	Open	03/22/2018
HTTP DoS	Cloud Storage	Very High	Open	03/22/2018
Weak Identity, Credential and Access Management	Cloud Storage	Very High	Open	03/22/2018
DDOS	Cloud Storage	Very High	Open	03/22/2018
Leveraging or Manipulating Configuration File Search Paths	Configuration File	Very High	Open	03/22/2018
Manipulating Writeable Configuration Files	Configuration File	Very High	Open	03/22/2018
Malware Propagation via USB Stick	USB Port	Very High	Open	03/22/2018
DEPRECATED: Malware Propagation via USB U3 Autorun	USB Port	Very High	Open	03/22/2018
DEPRECATED: Malware Propagation via Infected Peripheral Device	USB Port	Very High	Open	03/22/2018
USB Memory Attacks	USB Port	High	Open	03/22/2018
Sensitive Data Exposure	Observation Center	Very High	Open	03/22/2018
Sensitive Data Exposure	Hospital	Very High	Open	03/22/2018
Malware Propagation via USB Stick	USB	Very High	Open	03/22/2018
DEPRECATED: Malware Propagation via USB U3 Autorun	USB	Very High	Open	03/22/2018
DEPRECATED: Malware Propagation via Infected Peripheral Device	USB	Very High	Open	03/22/2018
USB Memory Attacks	USB	High	Open	03/22/2018
TCP SYN Scan	TCP	Low	Open	03/22/2018
TCP Window Scan	TCP	Low	Open	03/22/2018
TCP RPC Scan	TCP	Low	Open	03/22/2018
TCP Sequence Number Probe	TCP	Low	Open	03/22/2018
TCP ISN Greatest Common Divisor Probe	TCP	Low	Open	03/22/2018
TCP ISN Counter Rate Probe	TCP	Low	Open	03/22/2018
TCP ISN Sequence Predictability Probe	TCP	Low	Open	03/22/2018
TCP Congestion Control Flag Probe	TCP	Low	Open	03/22/2018
TCP Initial Window Size Probe	TCP	Low	Open	03/22/2018
Media Access Control - MAC Attack	VLAN	Very	Open	03/22/2018

		High		
Double Encapsulation VLAN Hopping Attack	VLAN	Very High	Open	03/22/2018
Address Resolution Protocol - ARP Attacks	VLAN	Very High	Open	03/22/2018
Spanning Tree Attack	VLAN	Very High	Open	03/22/2018
VLAN Trunking Protocol - VTP attack	VLAN	Very High	Open	03/22/2018
Cisco Discovery Protocol - CDP Attacks	VLAN	Very High	Open	03/22/2018
Private VLAN - PVLAN Attack	VLAN	Very High	Open	03/22/2018
Basic VLAN Hopping attack	VLAN	Very High	Open	03/22/2018
VMPS and or VQP attack	VLAN	Very High	Open	03/22/2018
Session Hijacking	VHF	Very High	Open	03/22/2018
Protocol Analysis	VHF	Low	Open	03/22/2018
External Entity Attack	VHF	Medium	Open	03/22/2018
Denial of Service through Resource Depletion	VHF	Medium	Open	03/22/2018
Protocol Manipulation	VHF	Medium	Open	03/22/2018
Traceroute Route Enumeration	VHF	Low	Open	03/22/2018
Content Spoofing	3G	Medium	Open	03/22/2018
Sniffing Attacks	3G	Medium	Open	03/22/2018
Action Spoofing	3G	Very High	Open	03/22/2018
Denial of Service through Resource Depletion	3G	Medium	Open	03/22/2018
Privilege Abuse	3G	Very High	Open	03/22/2018
Resource Location Spoofing	3G	Very High	Open	03/22/2018
Sniffing Network Traffic	3G	Very High	Open	03/22/2018
Intent Spoof	3G	Very High	Open	03/22/2018
Cellular Traffic Intercept	3G	Very High	Open	03/22/2018
Denial of Service	3G	Very High	Open	03/22/2018
Exploiting Incorrectly Configured SSL	HTTPS	Very High	Open	03/22/2018
Man in the Middle Attack	Bluetooth	Very High	Open	03/22/2018
Sniffing Attacks	ZigBee	Medium	Open	03/22/2018
Man in the Middle Attack	ZigBee	Very High	Open	03/22/2018
Add Malicious File to Shared Webroot	ZigBee	Very High	Open	03/22/2018
Shared Technology Issues	ZigBee	Very High	Open	03/22/2018
Man in the Middle Attack	WiFi	Very	Open	03/22/2018

		High		
Wi-Fi Jamming	WiFi	High	Open	03/22/2018
WiFi MAC Address Tracking	WiFi	Very High	Open	03/22/2018
WiFi SSID Tracking	WiFi	Very High	Open	03/22/2018
Email Injection	IMAP	Medium	Open	03/22/2018
IMAP or SMTP Command Injection	IMAP	Medium	Open	03/22/2018
Exploitation of Authorization	4G	Medium	Open	03/22/2018
Identity Spoofing - Impersonation	4G	Medium	Open	03/22/2018
Sniffing Attacks	4G	Medium	Open	03/22/2018
Exploitation of Authentication	4G	Very High	Open	03/22/2018
Denial of Service	4G	Very High	Open	03/22/2018
Authentication Bypass	Sensors	Medium	Open	03/22/2018
White Box Reverse Engineering	Observation Center	Medium	Open	03/22/2018
White Box Reverse Engineering	Hospital	Medium	Open	03/22/2018
Denial of Service	Cloud Storage	Very High	Open	03/22/2018
White Box Reverse Engineering	Cloud Storage	Medium	Open	03/22/2018
Encryption Brute Forcing	Cloud Storage	Low	Open	03/22/2018
Denial of Service through Resource Depletion	Cloud Server	Medium	Open	03/22/2018
Hijacking a Privileged Thread of Execution	Cloud Server	Very High	Open	03/22/2018
Denial of Service	Cloud Server	Very High	Open	03/22/2018
DDOS	Cloud Server	Very High	Open	03/22/2018
White Box Reverse Engineering	Cloud Server	Medium	Open	03/22/2018
Sensitive Data Exposure	Cloud Server	Very High	Open	03/22/2018
Encryption Brute Forcing	Cloud Server	Low	Open	03/22/2018
Weak Identity, Credential and Access Management	Data Storage and Processing	Very High	Open	03/22/2018
Denial of Service	Data Storage and Processing	Very High	Open	03/22/2018
Malicious Insiders	Data Storage and Processing	Very High	Open	03/22/2018
Account Hijacking	Data Storage and Processing	Very High	Open	03/22/2018
System and Application Vulnerability	Data Storage and Processing	Very High	Open	03/22/2018
Confidential Data Exposure	Data Storage and Processing	Very High	Open	03/22/2018
Insecure Communication	Data Storage and Processing	Very High	Open	03/22/2018
Permanent Data Loss	Data Storage and Processing	Very High	Open	03/22/2018
Code Injection	Data Storage and Processing	High	Open	03/22/2018
Reflected Cross Site Scripting - WASC	Data Storage and	High	Open	03/22/2018

	Processing			
Clickjacking	Data Storage and Processing	Very High	Open	03/22/2018
Cross Site Request Forgery	Data Storage and Processing	Very High	Open	03/22/2018
SQL Injection	Data Storage and Processing	High	Open	03/22/2018
Blind SQL Injection	Data Storage and Processing	High	Open	03/22/2018
Persistent Cross Site Scripting - WASC	Data Storage and Processing	High	Open	03/22/2018
Accessing, Intercepting, Modifying HTTP Cookies	Data Storage and Processing	High	Open	03/22/2018
Session Hijacking	Data Storage and Processing	Very High	Open	03/22/2018
Session Credential Falsification through Forging	Data Storage and Processing	Medium	Open	03/22/2018
Reusing Session IDs aka Session Replay	Data Storage and Processing	High	Open	03/22/2018
Session Fixation	Data Storage and Processing	High	Open	03/22/2018
Overflow Buffers	Data Storage and Processing	Very High	Open	03/22/2018
File System Function Injection, Content Based	Data Storage and Processing	Very High	Open	03/22/2018
Leverage Executable Code in Non-Executable Files	Data Storage and Processing	Very High	Open	03/22/2018
Leveraging or Manipulating Configuration File Search Paths	Data Storage and Processing	Very High	Open	03/22/2018
Overflow Binary Resource File	Data Storage and Processing	Very High	Open	03/22/2018
Manipulating Writeable Configuration Files	Data Storage and Processing	Very High	Open	03/22/2018
Manipulating Web Input to File System Calls	Data Storage and Processing	Very High	Open	03/22/2018
Authentication Bypass	Sensor Data	Medium	Open	03/22/2018
Authentication Bypass	Sensors	Medium	Open	03/22/2018
White Box Reverse Engineering	Other Services	Medium	Open	03/22/2018
Authentication Bypass	Wi-Fi Port	Medium	Open	03/22/2018
Authentication Bypass	Control Data	Medium	Open	03/22/2018
White Box Reverse Engineering	Labs	Medium	Open	03/22/2018
Authentication Bypass	Sensors	Medium	Open	03/22/2018
Authentication Bypass	Sensors	Medium	Open	03/22/2018
Man in the Middle Attack	Satellite System	Very High	Open	03/21/2018
Session Hijacking	Satellite System	Very High	Open	03/21/2018
Session Credential Falsification through Forging	Satellite System	Medium	Open	03/21/2018
Exploitation of Trusted Credentials	Satellite System	High	Open	03/21/2018
WS: Insufficient Authentication	Satellite System	Very High	Open	03/21/2018
Exploitation of Authentication	Satellite System	Very High	Open	03/21/2018

Privilege Escalation	Satellite System	Very High	Open	03/21/2018
Lack of confidentiality	Satellite System	Very High	Open	03/21/2018
Sensitive Data Exposure	Satellite System	Very High	Open	03/21/2018
SQL Injection	Satellite System	High	Open	03/21/2018
Blind SQL Injection	Satellite System	High	Open	03/21/2018
Sensitive Data Exposure	Satellite System	Very High	Open	03/21/2018
HTTP DoS	Satellite System	Very High	Open	03/21/2018
Weak Identity, Credential and Access Management	Satellite System	Very High	Open	03/21/2018
DDOS	Satellite System	Very High	Open	03/21/2018
Session Hijacking	Satellite System	Very High	Open	03/21/2018
Denial of Service through Resource Depletion	Satellite System	Medium	Open	03/21/2018
Protocol Manipulation	Satellite System	Medium	Open	03/21/2018
TCP SYN Scan	Satellite System	Low	Open	03/21/2018
TCP ACK Ping	Satellite System	Low	Open	03/21/2018
TCP SYN Ping	Satellite System	Low	Open	03/21/2018
TCP Connect Scan	Satellite System	Low	Open	03/21/2018
TCP ACK Scan	Satellite System	Low	Open	03/21/2018
Exploit Common or default Usernames and Passwords	Satellite System	High	Open	03/21/2018
WS: XML Denial of Service	Satellite System	Very High	Open	03/21/2018
Gather Information	Satellite System	Very High	Open	03/21/2018
HTTP DoS	Satellite System	Very High	Open	03/21/2018
ICMP Fragmentation	Satellite System	Very High	Open	03/21/2018
Unauthorized Use of Device Resources	Satellite System	Very High	Open	03/21/2018
Denial of Service	Satellite System	Very High	Open	03/21/2018
Eavesdropping	Satellite System	Very High	Open	03/21/2018
Reusing Session IDs aka Session Replay	Satellite System	High	Open	03/21/2018
Protocol Manipulation	Satellite System	Medium	Open	03/21/2018
Lifting Data Embedded in Client Distributions	Satellite System	Very High	Open	03/21/2018
Password Recovery Exploitation	Satellite System	High	Open	03/21/2018
Manipulate Resources	Satellite System	Very High	Open	03/21/2018
Jamming	Satellite System	Very High	Open	03/21/2018
Jamming	Satellite System	Very High	Open	03/21/2018
Denial of Service	Satellite System	Very High	Open	03/21/2018

Eavesdropping	Satellite System	Very High	Open	03/21/2018
Hijacking	Satellite System	Very High	Open	03/21/2018
TCP SYN Scan	Satellite System	Low	Open	03/21/2018
TCP Window Scan	Satellite System	Low	Open	03/21/2018
TCP RPC Scan	Satellite System	Low	Open	03/21/2018
TCP Sequence Number Probe	Satellite System	Low	Open	03/21/2018
TCP ISN Greatest Common Divisor Probe	Satellite System	Low	Open	03/21/2018
TCP ISN Counter Rate Probe	Satellite System	Low	Open	03/21/2018
TCP ISN Sequence Predictability Probe	Satellite System	Low	Open	03/21/2018
TCP Congestion Control Flag Probe	Satellite System	Low	Open	03/21/2018
TCP Initial Window Size Probe	Satellite System	Low	Open	03/21/2018
Exploiting Incorrectly Configured SSL	Satellite System	Very High	Open	03/21/2018
Media Access Control - MAC Attack	Satellite System	Very High	Open	03/21/2018
Double Encapsulation VLAN Hopping Attack	Satellite System	Very High	Open	03/21/2018
Address Resolution Protocol - ARP Attacks	Satellite System	Very High	Open	03/21/2018
Spanning Tree Attack	Satellite System	Very High	Open	03/21/2018
VLAN Trunking Protocol - VTP attack	Satellite System	Very High	Open	03/21/2018
Cisco Discovery Protocol - CDP Attacks	Satellite System	Very High	Open	03/21/2018
Private VLAN - PVLAN Attack	Satellite System	Very High	Open	03/21/2018
Basic VLAN Hopping attack	Satellite System	Very High	Open	03/21/2018
VMPS and or VQP attack	Satellite System	Very High	Open	03/21/2018
Malware Propagation via USB Stick	Satellite System	Very High	Open	03/21/2018
DEPRECATED: Malware Propagation via USB U3 Autorun	Satellite System	Very High	Open	03/21/2018
DEPRECATED: Malware Propagation via Infected Peripheral Device	Satellite System	Very High	Open	03/21/2018
USB Memory Attacks	Satellite System	High	Open	03/21/2018
Content Spoofing	Satellite System	Medium	Open	03/21/2018
Sniffing Attacks	Satellite System	Medium	Open	03/21/2018
Action Spoofing	Satellite System	Very High	Open	03/21/2018
Denial of Service through Resource Depletion	Satellite System	Medium	Open	03/21/2018
Privilege Abuse	Satellite System	Very High	Open	03/21/2018
Resource Location Spoofing	Satellite System	Very High	Open	03/21/2018
Sniffing Network Traffic	Satellite System	Very High	Open	03/21/2018
Intent Spoof	Satellite System	Very	Open	03/21/2018

		High		
Cellular Traffic Intercept	Satellite System	Very High	Open	03/21/2018
Denial of Service	Satellite System	Very High	Open	03/21/2018
Exploitation of Authorization	Satellite System	Medium	Open	03/21/2018
Identity Spoofing - Impersonation	Satellite System	Medium	Open	03/21/2018
Sniffing Attacks	Satellite System	Medium	Open	03/21/2018
Exploitation of Authentication	Satellite System	Very High	Open	03/21/2018
Denial of Service	Satellite System	Very High	Open	03/21/2018
File Manipulation	Satellite System	Medium	Open	03/21/2018
Accessing, Modifying or Executing Executable Files	Satellite System	Very High	Open	03/21/2018
Create files with the same name as files protected with a higher classification	Satellite System	Very High	Open	03/21/2018
Force Use of Corrupted Files	Satellite System	Medium	Open	03/21/2018
Leveraging or Manipulating Configuration File Search Paths	Satellite System	Very High	Open	03/21/2018
User-Controlled Filename	Satellite System	High	Open	03/21/2018
Manipulating Web Input to File System Calls	Satellite System	Very High	Open	03/21/2018
Identity Spoofing - Impersonation	Satellite System	Medium	Open	03/21/2018
Man in the Middle Attack	Satellite System	Very High	Open	03/21/2018
Targeted Malware	Satellite System	Very High	Open	03/21/2018
Account Footprinting	Satellite System	Very High	Open	03/21/2018
Wi-Fi Jamming	Satellite System	High	Open	03/21/2018
WiFi MAC Address Tracking	Satellite System	Very High	Open	03/21/2018
WiFi SSID Tracking	Satellite System	Very High	Open	03/21/2018
Malware Propagation via USB Stick	Satellite System	Very High	Open	03/21/2018
DEPRECATED: Malware Propagation via USB U3 Autorun	Satellite System	Very High	Open	03/21/2018
DEPRECATED: Malware Propagation via Infected Peripheral Device	Satellite System	Very High	Open	03/21/2018
USB Memory Attacks	Satellite System	High	Open	03/21/2018
Malicious Software Download	Satellite System	Very High	Open	03/21/2018
Content Spoofing	Satellite System	Medium	Open	03/21/2018
Protocol Manipulation	Satellite System	Medium	Open	03/21/2018
Physical Theft	Satellite System	Very High	Open	03/21/2018
Sensitive Data Exposure	Satellite System	Very High	Open	03/21/2018
Brute Force	Satellite System	High	Open	03/21/2018
Password Brute Forcing	Satellite System	High	Open	03/21/2018

Reusing Session IDs aka Session Replay	Satellite System	High	Open	03/21/2018
Denial of Service	Satellite System	Very High	Open	03/21/2018
Verify - Spoofed packet injection	Satellite System	Very High	Open	03/21/2018
SQL Injection	Satellite System	High	Open	03/21/2018
Blind SQL Injection	Satellite System	High	Open	03/21/2018
Session Hijacking	Satellite System	Very High	Open	03/21/2018
Denial of Service through Resource Depletion	Satellite System	Medium	Open	03/21/2018
TCP SYN Scan	Satellite System	Low	Open	03/21/2018
TCP ACK Ping	Satellite System	Low	Open	03/21/2018
TCP SYN Ping	Satellite System	Low	Open	03/21/2018
TCP Connect Scan	Satellite System	Low	Open	03/21/2018
TCP ACK Scan	Satellite System	Low	Open	03/21/2018
Exploit Common or default Usernames and Passwords	Satellite System	High	Open	03/21/2018
WS: XML Denial of Service	Satellite System	Very High	Open	03/21/2018
Gather Information	Satellite System	Very High	Open	03/21/2018
HTTP DoS	Satellite System	Very High	Open	03/21/2018
ICMP Fragmentation	Satellite System	Very High	Open	03/21/2018
Unauthorized Use of Device Resources	Satellite System	Very High	Open	03/21/2018
Eavesdropping	Satellite System	Very High	Open	03/21/2018
Reusing Session IDs aka Session Replay	Satellite System	High	Open	03/21/2018
Encryption Brute Forcing	Satellite System	Low	Open	03/21/2018
Clickjacking	Satellite System	Very High	Open	03/21/2018
Cross Site Request Forgery	Satellite System	Very High	Open	03/21/2018
SQL Injection	Satellite System	High	Open	03/21/2018
Blind SQL Injection	Satellite System	High	Open	03/21/2018
Reflected Cross Site Scripting - WASC	Satellite System	High	Open	03/21/2018
Persistent Cross Site Scripting - WASC	Satellite System	High	Open	03/21/2018
Accessing, Intercepting, Modifying HTTP Cookies	Satellite System	High	Open	03/21/2018
Email Injection	Satellite System	Medium	Open	03/21/2018
IMAP or SMTP Command Injection	Satellite System	Medium	Open	03/21/2018
File Manipulation	Satellite System	Medium	Open	03/21/2018
Accessing, Modifying or Executing Executable Files	Satellite System	Very High	Open	03/21/2018
Create files with the same name as files protected with a higher classification	Satellite System	Very High	Open	03/21/2018
Manipulating Writeable Configuration Files	Satellite System	Very High	Open	03/21/2018
Manipulating Web Input to File System Calls	Satellite System	Very High	Open	03/21/2018
Malware Infection into Product Software	Satellite System	Very	Open	03/21/2018

		High		
Session Hijacking	Satellite System	Very High	Open	03/21/2018
Session Credential Falsification through Forging	Satellite System	Medium	Open	03/21/2018
Reusing Session IDs aka Session Replay	Satellite System	High	Open	03/21/2018
Session Fixation	Satellite System	High	Open	03/21/2018
File Manipulation	Endpoint Security	Medium	Open	03/20/2018
Accessing, Modifying or Executing Executable Files	Endpoint Security	Very High	Open	03/20/2018
Create files with the same name as files protected with a higher classification	Endpoint Security	Very High	Open	03/20/2018
Force Use of Corrupted Files	Endpoint Security	Medium	Open	03/20/2018
Leveraging or Manipulating Configuration File Search Paths	Endpoint Security	Very High	Open	03/20/2018
User-Controlled Filename	Endpoint Security	High	Open	03/20/2018
Manipulating Web Input to File System Calls	Endpoint Security	Very High	Open	03/20/2018
Malware Propagation via USB Stick	Endpoint Security	Very High	Open	03/20/2018
DEPRECATED: Malware Propagation via USB U3 Autorun	Endpoint Security	Very High	Open	03/20/2018
DEPRECATED: Malware Propagation via Infected Peripheral Device	Endpoint Security	Very High	Open	03/20/2018
USB Memory Attacks	Endpoint Security	High	Open	03/20/2018
Overflow Buffers	Endpoint Security	Very High	Open	03/20/2018
Bluejacking	Endpoint Security	Very High	Open	03/20/2018
Bluesnarfing	Endpoint Security	Very High	Open	03/20/2018
Bluebugging	Endpoint Security	Very High	Open	03/20/2018
Man in the Middle Attack	Endpoint Security	Very High	Open	03/20/2018
Wi-Fi Jamming	Endpoint Security	High	Open	03/20/2018
WiFi MAC Address Tracking	Endpoint Security	Very High	Open	03/20/2018
WiFi SSID Tracking	Endpoint Security	Very High	Open	03/20/2018
Physical Theft	Endpoint Security	Very High	Open	03/20/2018
Jamming	Endpoint Security	Very High	Open	03/20/2018
Exploiting Incorrectly Configured SSL	Endpoint Security	Very High	Open	03/20/2018
Man in the Middle Attack	Endpoint Security	Very High	Open	03/20/2018
Wi-Fi Jamming	Endpoint Security	High	Open	03/20/2018
WiFi MAC Address Tracking	Endpoint Security	Very High	Open	03/20/2018
WiFi SSID Tracking	Endpoint Security	Very High	Open	03/20/2018
File Manipulation	Endpoint Security	Medium	Open	03/20/2018

Accessing, Modifying or Executing Executable Files	Endpoint Security	Very High	Open	03/20/2018
Create files with the same name as files protected with a higher classification	Endpoint Security	Very High	Open	03/20/2018
Manipulating Web Input to File System Calls	Endpoint Security	Very High	Open	03/20/2018
TCP SYN Scan	Endpoint Security	Low	Open	03/20/2018
TCP Window Scan	Endpoint Security	Low	Open	03/20/2018
TCP RPC Scan	Endpoint Security	Low	Open	03/20/2018
TCP Sequence Number Probe	Endpoint Security	Low	Open	03/20/2018
TCP ISN Greatest Common Divisor Probe	Endpoint Security	Low	Open	03/20/2018
TCP ISN Counter Rate Probe	Endpoint Security	Low	Open	03/20/2018
TCP ISN Sequence Predictability Probe	Endpoint Security	Low	Open	03/20/2018
TCP Congestion Control Flag Probe	Endpoint Security	Low	Open	03/20/2018
TCP Initial Window Size Probe	Endpoint Security	Low	Open	03/20/2018
Email Injection	Endpoint Security	Medium	Open	03/20/2018
DNS Cache Poisoning	Endpoint Security	Very High	Open	03/20/2018
Phishing	Endpoint Security	Very High	Open	03/20/2018
Targeted Malware	Endpoint Security	Very High	Open	03/20/2018
SPAM	Endpoint Security	Medium	Open	03/20/2018
Man in the Middle Attack	Endpoint Security	Very High	Open	03/20/2018
File Manipulation	Endpoint Security	Medium	Open	03/20/2018
Accessing, Modifying or Executing Executable Files	Endpoint Security	Very High	Open	03/20/2018
Create files with the same name as files protected with a higher classification	Endpoint Security	Very High	Open	03/20/2018
Manipulating Web Input to File System Calls	Endpoint Security	Very High	Open	03/20/2018
Identity Spoofing - Impersonation	Endpoint Security	Medium	Open	03/20/2018
Man in the Middle Attack	Endpoint Security	Very High	Open	03/20/2018
Targeted Malware	Endpoint Security	Very High	Open	03/20/2018
Account Footprinting	Endpoint Security	Very High	Open	03/20/2018
Email Injection	Endpoint Security	Medium	Open	03/21/2018
IMAP or SMTP Command Injection	Endpoint Security	Medium	Open	03/21/2018
IMAP or SMTP Command Injection	Endpoint Security	Medium	Open	03/21/2018
White Box Reverse Engineering	Endpoint Security	Medium	Open	03/21/2018
Sensitive Data Exposure	Endpoint Security	Very High	Open	03/21/2018
Email Injection	Endpoint Security	Medium	Open	03/21/2018
IMAP or SMTP Command Injection	Endpoint Security	Medium	Open	03/21/2018
Dictionary-based Password Attack	Endpoint Security	High	Open	03/21/2018
Password Brute Forcing	Endpoint Security	High	Open	03/21/2018
Password Recovery Exploitation	Endpoint Security	High	Open	03/21/2018

Exploit Common or default Usernames and Passwords	Endpoint Security	High	Open	03/21/2018
Cross Site Request Forgery	Endpoint Security	Very High	Open	03/21/2018
Reflected Cross Site Scripting - WASC	Endpoint Security	High	Open	03/21/2018
Dictionary-based Password Attack	Endpoint Security	High	Open	03/21/2018
Password Brute Forcing	Endpoint Security	High	Open	03/21/2018
Password Recovery Exploitation	Endpoint Security	High	Open	03/21/2018
Exploit Common or default Usernames and Passwords	Endpoint Security	High	Open	03/21/2018
Cross Site Request Forgery	Endpoint Security	Very High	Open	03/21/2018
Reflected Cross Site Scripting - WASC	Endpoint Security	High	Open	03/21/2018
Leveraging or Manipulating Configuration File Search Paths	Endpoint Security	Very High	Open	03/21/2018
Manipulating Writeable Configuration Files	Endpoint Security	Very High	Open	03/21/2018
Overflow Buffers	Endpoint Security	Very High	Open	03/21/2018
Verify - Insecure Configuration	Endpoint Security	Very High	Open	03/21/2018
DNS Cache Poisoning	Endpoint Security	Very High	Open	03/21/2018
Redirect Access to Libraries	Endpoint Security	Very High	Open	03/21/2018
Accessing, Modifying or Executing Executable Files	Endpoint Security	Very High	Open	03/21/2018
Code Inclusion	Endpoint Security	Very High	Open	03/21/2018
Malicious Software Download	Endpoint Security	Very High	Open	03/21/2018
File System Function Injection, Content Based	Endpoint Security	Very High	Open	03/21/2018
Hijacking a Privileged Thread of Execution	Endpoint Security	Very High	Open	03/21/2018
Overflow Binary Resource File	Endpoint Security	Very High	Open	03/21/2018
Malicious Logic Inserted Into Product	Endpoint Security	Very High	Open	03/21/2018
Malicious Logic Inserted Into Product Software by Authorized Developer	Endpoint Security	Very High	Open	03/21/2018
Malicious Logic Insertion into Product Software via Externally Manipulated Component	Endpoint Security	Very High	Open	03/21/2018
Malicious Logic Insertion into Product Software via Configuration Management Manipulation	Endpoint Security	Very High	Open	03/21/2018
Malicious Logic Insertion into Product Software via Inclusion of 3rd Party Component Dependency	Endpoint Security	Very High	Open	03/21/2018
Malicious Logic Insertion into Product Software during Update	Endpoint Security	Very High	Open	03/21/2018
Malware Infection into Product Software	Endpoint Security	Very High	Open	03/21/2018
Malware Propagation via USB Stick	Endpoint Security	Very High	Open	03/21/2018
Privilege Abuse	Endpoint Security	Very High	Open	03/21/2018
Buffer Manipulation	Endpoint Security	Very	Open	03/21/2018

		High		
Overread Buffers	Endpoint Security	Very High	Open	03/21/2018
Privilege Escalation	Endpoint Security	Very High	Open	03/21/2018
Malware-Directed Internal Reconnaissance	Endpoint Security	Very High	Open	03/21/2018
Targeted Malware	Endpoint Security	Very High	Open	03/21/2018
Install Rootkit	Endpoint Security	Very High	Open	03/21/2018
Malware Infection into Product Software	Endpoint Security	Very High	Open	03/21/2018
Man in the Middle Attack	Endpoint Security	Very High	Open	03/21/2018
iOS: Data Storage	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Weak Server Side Controls	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Insufficient Transport Layer Protection	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Client Side Injection	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Poor Authorization and Authentication	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Improper Session Handling	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Security Decisions via Untrusted Inputs	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Side Channel Data Leakage	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Broken Encryption	Telecom Network 3G	Very High	Open	03/19/2018
iOS: Sensitive Information Disclosure	Telecom Network 3G	Very High	Open	03/19/2018
Probe iOS Screenshots	Telecom Network 3G	Very High	Open	03/19/2018
Altered Installed BIOS	Telecom Network 3G	Very High	Open	03/19/2018
Physical Theft	Telecom Network 3G	Very High	Open	03/19/2018
Session Hijacking	Telecom Network 3G	Very High	Open	03/19/2018
Denial of Service through Resource Depletion	Telecom Network 3G	Medium	Open	03/19/2018
Protocol Manipulation	Telecom Network 3G	Medium	Open	03/19/2018
TCP SYN Scan	Telecom Network 3G	Low	Open	03/19/2018
TCP ACK Ping	Telecom Network 3G	Low	Open	03/19/2018
TCP SYN Ping	Telecom Network 3G	Low	Open	03/19/2018
TCP Connect Scan	Telecom Network 3G	Low	Open	03/19/2018
TCP ACK Scan	Telecom Network 3G	Low	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network 3G	High	Open	03/19/2018
WS: XML Denial of Service	Telecom Network 3G	Very High	Open	03/19/2018
Gather Information	Telecom Network 3G	Very	Open	03/19/2018

		High		
HTTP DoS	Telecom Network 3G	Very High	Open	03/19/2018
ICMP Fragmentation	Telecom Network 3G	Very High	Open	03/19/2018
Unauthorized Use of Device Resources	Telecom Network 3G	Very High	Open	03/19/2018
Denial of Service	Telecom Network 3G	Very High	Open	03/19/2018
Eavesdropping	Telecom Network 3G	Very High	Open	03/19/2018
Reusing Session IDs aka Session Replay	Telecom Network 3G	High	Open	03/19/2018
Weak Identity, Credential and Access Management	Telecom Network 3G	Very High	Open	03/19/2018
Denial of Service	Telecom Network 3G	Very High	Open	03/19/2018
Sensitive Data Exposure	Telecom Network 3G	Very High	Open	03/19/2018
Code Injection	Telecom Network 3G	High	Open	03/19/2018
Reflected Cross Site Scripting - WASC	Telecom Network 3G	High	Open	03/19/2018
Encryption Brute Forcing	Telecom Network 3G	Low	Open	03/19/2018
Cross Site Request Forgery	Telecom Network 3G	Very High	Open	03/19/2018
Overflow Buffers	Telecom Network 3G	Very High	Open	03/19/2018
Sensitive Data Exposure	Telecom Network 3G	Very High	Open	03/19/2018
Weak Identity, Credential and Access Management	Telecom Network 3G	Very High	Open	03/19/2018
Denial of Service	Telecom Network 3G	Very High	Open	03/19/2018
Code Injection	Telecom Network 3G	High	Open	03/19/2018
Reflected Cross Site Scripting - WASC	Telecom Network 3G	High	Open	03/19/2018
Dictionary-based Password Attack	Telecom Network 3G	High	Open	03/19/2018
Password Brute Forcing	Telecom Network 3G	High	Open	03/19/2018
Password Recovery Exploitation	Telecom Network 3G	High	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network 3G	High	Open	03/19/2018
Encryption Brute Forcing	Telecom Network 3G	Low	Open	03/19/2018
Cross Site Request Forgery	Telecom Network 3G	Very High	Open	03/19/2018
Overflow Buffers	Telecom Network 3G	Very High	Open	03/19/2018
Overflow Buffers	Telecom Network 3G	Very High	Open	03/19/2018
Cross Site Request Forgery	Telecom Network 3G	Very High	Open	03/19/2018
Dictionary-based Password Attack	Telecom Network 3G	High	Open	03/19/2018
Password Brute Forcing	Telecom Network 3G	High	Open	03/19/2018
Password Recovery Exploitation	Telecom Network 3G	High	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network 3G	High	Open	03/19/2018
Encryption Brute Forcing	Telecom Network 3G	Low	Open	03/19/2018

Weak Identity, Credential and Access Management	Telecom Network 3G	Very High	Open	03/19/2018
Denial of Service	Telecom Network 3G	Very High	Open	03/19/2018
Sensitive Data Exposure	Telecom Network 3G	Very High	Open	03/19/2018
Code Injection	Telecom Network 3G	High	Open	03/19/2018
Reflected Cross Site Scripting - WASC	Telecom Network 3G	High	Open	03/19/2018
Authentication Bypass	Telecom Network 3G	Medium	Open	03/19/2018
Sniff Application Code	Telecom Network 3G	High	Open	03/19/2018
Exploiting Incorrectly Configured SSL	Telecom Network 3G	Very High	Open	03/19/2018
Data Interception Attacks	Telecom Network 3G	Medium	Open	03/19/2018
Fake the Source of Data	Telecom Network 3G	Medium	Open	03/19/2018
User-Controlled Filename	Telecom Network 3G	High	Open	03/19/2018
Manipulating User State	Telecom Network 3G	High	Open	03/19/2018
Email Injection	Telecom Network 3G	Medium	Open	03/19/2018
IMAP or SMTP Command Injection	Telecom Network 3G	Medium	Open	03/19/2018
Content Spoofing	Telecom Network 3G	Medium	Open	03/20/2018
Action Spoofing	Telecom Network 3G	Very High	Open	03/20/2018
Resource Location Spoofing	Telecom Network 3G	Very High	Open	03/20/2018
Intent Spoof	Telecom Network 3G	Very High	Open	03/20/2018
Denial of Service through Resource Depletion	Telecom Network 3G	Medium	Open	03/20/2018
Denial of Service	Telecom Network 3G	Very High	Open	03/20/2018
Sniffing Attacks	Telecom Network 3G	Medium	Open	03/20/2018
Sniffing Network Traffic	Telecom Network 3G	Very High	Open	03/20/2018
Privilege Abuse	Telecom Network 3G	Very High	Open	03/20/2018
Cellular Traffic Intercept	Telecom Network 3G	Very High	Open	03/20/2018
SQL Injection	Telecom Network 3G	High	Open	03/20/2018
SQL Injection	Telecom Network 3G	High	Open	03/20/2018
SQL Injection	Telecom Network 3G	High	Open	03/20/2018
Blind SQL Injection	Telecom Network 3G	High	Open	03/20/2018
Blind SQL Injection	Telecom Network 3G	High	Open	03/20/2018
Blind SQL Injection	Telecom Network 3G	High	Open	03/20/2018
Persistent Cross Site Scripting - WASC	Telecom Network 3G	High	Open	03/20/2018
Persistent Cross Site Scripting - WASC	Telecom Network 3G	High	Open	03/20/2018
Persistent Cross Site Scripting - WASC	Telecom Network 3G	High	Open	03/20/2018
Clickjacking	Telecom Network 3G	Very High	Open	03/20/2018
Clickjacking	Telecom Network 3G	Very High	Open	03/20/2018
Clickjacking	Telecom Network 3G	Very High	Open	03/20/2018

CVE-2015-0726	Telecom Network 3G	Very High	Open	03/19/2018
CVE-2016-6375	Telecom Network 3G	Very High	Open	03/19/2018
CVE-2015-0726	Telecom Network 3G	Very High	Open	03/19/2018
CVE-2016-6375	Telecom Network 3G	Very High	Open	03/19/2018
CVE-2005-0356	Telecom Network 3G	Very High	Open	03/19/2018
CVE-2005-4499	Telecom Network 3G	Very High	Open	03/19/2018
CVE-2006-4098	Telecom Network 3G	Very High	Open	03/19/2018
File Manipulation	Telecom Network Core	Medium	Open	03/19/2018
Accessing, Modifying or Executing Executable Files	Telecom Network Core	Very High	Open	03/19/2018
Create files with the same name as files protected with a higher classification	Telecom Network Core	Very High	Open	03/19/2018
Manipulating Web Input to File System Calls	Telecom Network Core	Very High	Open	03/19/2018
Authentication Bypass	Telecom Network Core	Medium	Open	03/19/2018
Sniff Application Code	Telecom Network Core	High	Open	03/19/2018
Sensitive Data Exposure	Telecom Network Core	Very High	Open	03/19/2018
Weak Identity, Credential and Access Management	Telecom Network Core	Very High	Open	03/19/2018
Denial of Service	Telecom Network Core	Very High	Open	03/19/2018
Code Injection	Telecom Network Core	High	Open	03/19/2018
Reflected Cross Site Scripting - WASC	Telecom Network Core	High	Open	03/19/2018
Dictionary-based Password Attack	Telecom Network Core	High	Open	03/19/2018
Password Brute Forcing	Telecom Network Core	High	Open	03/19/2018
Password Recovery Exploitation	Telecom Network Core	High	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network Core	High	Open	03/19/2018
Encryption Brute Forcing	Telecom Network Core	Low	Open	03/19/2018
Cross Site Request Forgery	Telecom Network Core	Very High	Open	03/19/2018
Overflow Buffers	Telecom Network Core	Very High	Open	03/19/2018
Session Hijacking	Telecom Network Core	Very High	Open	03/19/2018
Denial of Service through Resource Depletion	Telecom Network Core	Medium	Open	03/19/2018
Protocol Manipulation	Telecom Network Core	Medium	Open	03/19/2018
TCP SYN Scan	Telecom Network Core	Low	Open	03/19/2018
TCP ACK Ping	Telecom Network Core	Low	Open	03/19/2018
TCP SYN Ping	Telecom Network Core	Low	Open	03/19/2018
TCP Connect Scan	Telecom Network Core	Low	Open	03/19/2018
TCP ACK Scan	Telecom Network Core	Low	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network Core	High	Open	03/19/2018
WS: XML Denial of Service	Telecom Network Core	Very	Open	03/19/2018

		High		
Gather Information	Telecom Network Core	Very High	Open	03/19/2018
HTTP DoS	Telecom Network Core	Very High	Open	03/19/2018
ICMP Fragmentation	Telecom Network Core	Very High	Open	03/19/2018
Unauthorized Use of Device Resources	Telecom Network Core	Very High	Open	03/19/2018
Denial of Service	Telecom Network Core	Very High	Open	03/19/2018
Eavesdropping	Telecom Network Core	Very High	Open	03/19/2018
Reusing Session IDs aka Session Replay	Telecom Network Core	High	Open	03/19/2018
Session Hijacking	Telecom Network Core	Very High	Open	03/19/2018
Denial of Service through Resource Depletion	Telecom Network Core	Medium	Open	03/19/2018
Protocol Manipulation	Telecom Network Core	Medium	Open	03/19/2018
TCP SYN Scan	Telecom Network Core	Low	Open	03/19/2018
TCP ACK Ping	Telecom Network Core	Low	Open	03/19/2018
TCP SYN Ping	Telecom Network Core	Low	Open	03/19/2018
TCP Connect Scan	Telecom Network Core	Low	Open	03/19/2018
TCP ACK Scan	Telecom Network Core	Low	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network Core	High	Open	03/19/2018
WS: XML Denial of Service	Telecom Network Core	Very High	Open	03/19/2018
Gather Information	Telecom Network Core	Very High	Open	03/19/2018
HTTP DoS	Telecom Network Core	Very High	Open	03/19/2018
ICMP Fragmentation	Telecom Network Core	Very High	Open	03/19/2018
Unauthorized Use of Device Resources	Telecom Network Core	Very High	Open	03/19/2018
Denial of Service	Telecom Network Core	Very High	Open	03/19/2018
Eavesdropping	Telecom Network Core	Very High	Open	03/19/2018
Reusing Session IDs aka Session Replay	Telecom Network Core	High	Open	03/19/2018
Session Hijacking	Telecom Network Core	Very High	Open	03/19/2018
Denial of Service through Resource Depletion	Telecom Network Core	Medium	Open	03/19/2018
Protocol Manipulation	Telecom Network Core	Medium	Open	03/19/2018
TCP SYN Scan	Telecom Network Core	Low	Open	03/19/2018
TCP ACK Ping	Telecom Network Core	Low	Open	03/19/2018
TCP SYN Ping	Telecom Network Core	Low	Open	03/19/2018
TCP Connect Scan	Telecom Network Core	Low	Open	03/19/2018
TCP ACK Scan	Telecom Network Core	Low	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network Core	High	Open	03/19/2018
WS: XML Denial of Service	Telecom Network Core	Very High	Open	03/19/2018

Gather Information	Telecom Network Core	Very High	Open	03/19/2018
HTTP DoS	Telecom Network Core	Very High	Open	03/19/2018
ICMP Fragmentation	Telecom Network Core	Very High	Open	03/19/2018
Unauthorized Use of Device Resources	Telecom Network Core	Very High	Open	03/19/2018
Denial of Service	Telecom Network Core	Very High	Open	03/19/2018
Eavesdropping	Telecom Network Core	Very High	Open	03/19/2018
Reusing Session IDs aka Session Replay	Telecom Network Core	High	Open	03/19/2018
Session Hijacking	Telecom Network Core	Very High	Open	03/19/2018
Denial of Service through Resource Depletion	Telecom Network Core	Medium	Open	03/19/2018
Protocol Manipulation	Telecom Network Core	Medium	Open	03/19/2018
TCP SYN Scan	Telecom Network Core	Low	Open	03/19/2018
TCP ACK Ping	Telecom Network Core	Low	Open	03/19/2018
TCP SYN Ping	Telecom Network Core	Low	Open	03/19/2018
TCP Connect Scan	Telecom Network Core	Low	Open	03/19/2018
TCP ACK Scan	Telecom Network Core	Low	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network Core	High	Open	03/19/2018
WS: XML Denial of Service	Telecom Network Core	Very High	Open	03/19/2018
Gather Information	Telecom Network Core	Very High	Open	03/19/2018
HTTP DoS	Telecom Network Core	Very High	Open	03/19/2018
ICMP Fragmentation	Telecom Network Core	Very High	Open	03/19/2018
Unauthorized Use of Device Resources	Telecom Network Core	Very High	Open	03/19/2018
Denial of Service	Telecom Network Core	Very High	Open	03/19/2018
Eavesdropping	Telecom Network Core	Very High	Open	03/19/2018
Reusing Session IDs aka Session Replay	Telecom Network Core	High	Open	03/19/2018
Exploiting Incorrectly Configured SSL	Telecom Network Core	Very High	Open	03/19/2018
Encryption Brute Forcing	Telecom Network Core	Low	Open	03/19/2018
SQL Injection	Telecom Network Core	High	Open	03/20/2018
Blind SQL Injection	Telecom Network Core	High	Open	03/20/2018
Persistent Cross Site Scripting - WASC	Telecom Network Core	High	Open	03/20/2018
Clickjacking	Telecom Network Core	Very High	Open	03/20/2018
iOS: Data Storage	Telecom Network 4G	Very High	Open	03/19/2018
iOS: Weak Server Side Controls	Telecom Network 4G	Very High	Open	03/19/2018
iOS: Insufficient Transport Layer Protection	Telecom Network 4G	Very High	Open	03/19/2018

iOS: Client Side Injection	Telecom Network 4G	Very High	Open	03/19/2018
iOS: Poor Authorization and Authentication	Telecom Network 4G	Very High	Open	03/19/2018
iOS: Improper Session Handling	Telecom Network 4G	Very High	Open	03/19/2018
iOS: Security Decisions via Untrusted Inputs	Telecom Network 4G	Very High	Open	03/19/2018
iOS: Side Channel Data Leakage	Telecom Network 4G	Very High	Open	03/19/2018
iOS: Broken Encryption	Telecom Network 4G	Very High	Open	03/19/2018
iOS: Sensitive Information Disclosure	Telecom Network 4G	Very High	Open	03/19/2018
Probe iOS Screenshots	Telecom Network 4G	Very High	Open	03/19/2018
Altered Installed BIOS	Telecom Network 4G	Very High	Open	03/19/2018
Session Hijacking	Telecom Network 4G	Very High	Open	03/19/2018
Denial of Service through Resource Depletion	Telecom Network 4G	Medium	Open	03/19/2018
Protocol Manipulation	Telecom Network 4G	Medium	Open	03/19/2018
TCP SYN Scan	Telecom Network 4G	Low	Open	03/19/2018
TCP ACK Ping	Telecom Network 4G	Low	Open	03/19/2018
TCP SYN Ping	Telecom Network 4G	Low	Open	03/19/2018
TCP Connect Scan	Telecom Network 4G	Low	Open	03/19/2018
TCP ACK Scan	Telecom Network 4G	Low	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network 4G	High	Open	03/19/2018
WS: XML Denial of Service	Telecom Network 4G	Very High	Open	03/19/2018
Gather Information	Telecom Network 4G	Very High	Open	03/19/2018
HTTP DoS	Telecom Network 4G	Very High	Open	03/19/2018
ICMP Fragmentation	Telecom Network 4G	Very High	Open	03/19/2018
Unauthorized Use of Device Resources	Telecom Network 4G	Very High	Open	03/19/2018
Denial of Service	Telecom Network 4G	Very High	Open	03/19/2018
Eavesdropping	Telecom Network 4G	Very High	Open	03/19/2018
Reusing Session IDs aka Session Replay	Telecom Network 4G	High	Open	03/19/2018
Physical Theft	Telecom Network 4G	Very High	Open	03/19/2018
Exploiting Incorrectly Configured SSL	Telecom Network 4G	Very High	Open	03/19/2018
Authentication Bypass	Telecom Network 4G	Medium	Open	03/19/2018
Sniff Application Code	Telecom Network 4G	High	Open	03/19/2018
Weak Identity, Credential and Access Management	Telecom Network 4G	Very High	Open	03/19/2018
Denial of Service	Telecom Network 4G	Very High	Open	03/19/2018

Sensitive Data Exposure	Telecom Network 4G	Very High	Open	03/19/2018
Code Injection	Telecom Network 4G	High	Open	03/19/2018
Reflected Cross Site Scripting - WASC	Telecom Network 4G	High	Open	03/19/2018
Encryption Brute Forcing	Telecom Network 4G	Low	Open	03/19/2018
Cross Site Request Forgery	Telecom Network 4G	Very High	Open	03/19/2018
Overflow Buffers	Telecom Network 4G	Very High	Open	03/19/2018
Sensitive Data Exposure	Telecom Network 4G	Very High	Open	03/19/2018
Weak Identity, Credential and Access Management	Telecom Network 4G	Very High	Open	03/19/2018
Denial of Service	Telecom Network 4G	Very High	Open	03/19/2018
Code Injection	Telecom Network 4G	High	Open	03/19/2018
Reflected Cross Site Scripting - WASC	Telecom Network 4G	High	Open	03/19/2018
Dictionary-based Password Attack	Telecom Network 4G	High	Open	03/19/2018
Password Brute Forcing	Telecom Network 4G	High	Open	03/19/2018
Password Recovery Exploitation	Telecom Network 4G	High	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network 4G	High	Open	03/19/2018
Encryption Brute Forcing	Telecom Network 4G	Low	Open	03/19/2018
Cross Site Request Forgery	Telecom Network 4G	Very High	Open	03/19/2018
Overflow Buffers	Telecom Network 4G	Very High	Open	03/19/2018
Weak Identity, Credential and Access Management	Telecom Network 4G	Very High	Open	03/19/2018
Denial of Service	Telecom Network 4G	Very High	Open	03/19/2018
Sensitive Data Exposure	Telecom Network 4G	Very High	Open	03/19/2018
Code Injection	Telecom Network 4G	High	Open	03/19/2018
Reflected Cross Site Scripting - WASC	Telecom Network 4G	High	Open	03/19/2018
Dictionary-based Password Attack	Telecom Network 4G	High	Open	03/19/2018
Password Brute Forcing	Telecom Network 4G	High	Open	03/19/2018
Password Recovery Exploitation	Telecom Network 4G	High	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network 4G	High	Open	03/19/2018
Encryption Brute Forcing	Telecom Network 4G	Low	Open	03/19/2018
Overflow Buffers	Telecom Network 4G	Very High	Open	03/19/2018
Cross Site Request Forgery	Telecom Network 4G	Very High	Open	03/19/2018
Exploitation of Authorization	Telecom Network 4G	Medium	Open	03/19/2018
Identity Spoofing - Impersonation	Telecom Network 4G	Medium	Open	03/19/2018
Sniffing Attacks	Telecom Network 4G	Medium	Open	03/19/2018
Exploitation of Authentication	Telecom Network 4G	Very High	Open	03/19/2018
Denial of Service	Telecom Network 4G	Very High	Open	03/19/2018
Man in the Middle Attack	Telecom Network 4G	Very	Open	03/19/2018

		High		
Wi-Fi Jamming	Telecom Network 4G	High	Open	03/19/2018
WiFi MAC Address Tracking	Telecom Network 4G	Very High	Open	03/19/2018
WiFi SSID Tracking	Telecom Network 4G	Very High	Open	03/19/2018
Data Interception Attacks	Telecom Network 4G	Medium	Open	03/19/2018
Fake the Source of Data	Telecom Network 4G	Medium	Open	03/19/2018
User-Controlled Filename	Telecom Network 4G	High	Open	03/19/2018
Manipulating User State	Telecom Network 4G	High	Open	03/19/2018
Email Injection	Telecom Network 4G	Medium	Open	03/19/2018
IMAP or SMTP Command Injection	Telecom Network 4G	Medium	Open	03/19/2018
SQL Injection	Telecom Network 4G	High	Open	03/20/2018
SQL Injection	Telecom Network 4G	High	Open	03/20/2018
SQL Injection	Telecom Network 4G	High	Open	03/20/2018
Blind SQL Injection	Telecom Network 4G	High	Open	03/20/2018
Blind SQL Injection	Telecom Network 4G	High	Open	03/20/2018
Blind SQL Injection	Telecom Network 4G	High	Open	03/20/2018
Persistent Cross Site Scripting - WASC	Telecom Network 4G	High	Open	03/20/2018
Persistent Cross Site Scripting - WASC	Telecom Network 4G	High	Open	03/20/2018
Persistent Cross Site Scripting - WASC	Telecom Network 4G	High	Open	03/20/2018
Clickjacking	Telecom Network 4G	Very High	Open	03/20/2018
Clickjacking	Telecom Network 4G	Very High	Open	03/20/2018
Clickjacking	Telecom Network 4G	Very High	Open	03/20/2018
Session Hijacking	Telecom Network IMS	Very High	Open	03/19/2018
Denial of Service through Resource Depletion	Telecom Network IMS	Medium	Open	03/19/2018
Protocol Manipulation	Telecom Network IMS	Medium	Open	03/19/2018
TCP SYN Scan	Telecom Network IMS	Low	Open	03/19/2018
TCP ACK Ping	Telecom Network IMS	Low	Open	03/19/2018
TCP SYN Ping	Telecom Network IMS	Low	Open	03/19/2018
TCP Connect Scan	Telecom Network IMS	Low	Open	03/19/2018
TCP ACK Scan	Telecom Network IMS	Low	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network IMS	High	Open	03/19/2018
WS: XML Denial of Service	Telecom Network IMS	Very High	Open	03/19/2018
Gather Information	Telecom Network IMS	Very High	Open	03/19/2018
HTTP DoS	Telecom Network IMS	Very High	Open	03/19/2018
ICMP Fragmentation	Telecom Network IMS	Very High	Open	03/19/2018
Unauthorized Use of Device Resources	Telecom Network IMS	Very High	Open	03/19/2018
Denial of Service	Telecom Network IMS	Very High	Open	03/19/2018

Eavesdropping	Telecom Network IMS	Very High	Open	03/19/2018
Reusing Session IDs aka Session Replay	Telecom Network IMS	High	Open	03/19/2018
Sensitive Data Exposure	Telecom Network IMS	Very High	Open	03/19/2018
Weak Identity, Credential and Access Management	Telecom Network IMS	Very High	Open	03/19/2018
Denial of Service	Telecom Network IMS	Very High	Open	03/19/2018
Code Injection	Telecom Network IMS	High	Open	03/19/2018
Reflected Cross Site Scripting - WASC	Telecom Network IMS	High	Open	03/19/2018
Dictionary-based Password Attack	Telecom Network IMS	High	Open	03/19/2018
Password Brute Forcing	Telecom Network IMS	High	Open	03/19/2018
Password Recovery Exploitation	Telecom Network IMS	High	Open	03/19/2018
Exploit Common or default Usernames and Passwords	Telecom Network IMS	High	Open	03/19/2018
Encryption Brute Forcing	Telecom Network IMS	Low	Open	03/19/2018
Cross Site Request Forgery	Telecom Network IMS	Very High	Open	03/19/2018
Overflow Buffers	Telecom Network IMS	Very High	Open	03/19/2018
Authentication Bypass	Telecom Network IMS	Medium	Open	03/19/2018
Sniff Application Code	Telecom Network IMS	High	Open	03/19/2018
File Manipulation	Telecom Network IMS	Medium	Open	03/19/2018
Accessing, Modifying or Executing Executable Files	Telecom Network IMS	Very High	Open	03/19/2018
Create files with the same name as files protected with a higher classification	Telecom Network IMS	Very High	Open	03/19/2018
Manipulating Web Input to File System Calls	Telecom Network IMS	Very High	Open	03/19/2018
File Manipulation	Telecom Network IMS	Medium	Open	03/19/2018
Accessing, Modifying or Executing Executable Files	Telecom Network IMS	Very High	Open	03/19/2018
Create files with the same name as files protected with a higher classification	Telecom Network IMS	Very High	Open	03/19/2018
Manipulating Web Input to File System Calls	Telecom Network IMS	Very High	Open	03/19/2018
Man in the Middle Attack	Telecom Network IMS	Very High	Open	03/19/2018
Exploitation of Authorization	Telecom Network IMS	Medium	Open	03/19/2018
Identity Spoofing - Impersonation	Telecom Network IMS	Medium	Open	03/19/2018
Sniffing Attacks	Telecom Network IMS	Medium	Open	03/19/2018
Denial of Service through Resource Depletion	Telecom Network IMS	Medium	Open	03/19/2018
Exploitation of Authentication	Telecom Network IMS	Very High	Open	03/19/2018
OS Fingerprinting	Telecom Network IMS	Very High	Open	03/19/2018
Targeted Malware	Telecom Network IMS	Very High	Open	03/19/2018
Exploiting Incorrectly Configured SSL	Telecom Network IMS	Very High	Open	03/19/2018
Data Interception Attacks	Telecom Network IMS	Medium	Open	03/19/2018

Fake the Source of Data	Telecom Network IMS	Medium	Open	03/19/2018
TCP SYN Scan	Telecom Network IMS	Low	Open	03/19/2018
TCP Window Scan	Telecom Network IMS	Low	Open	03/19/2018
TCP RPC Scan	Telecom Network IMS	Low	Open	03/19/2018
Resource Location Spoofing	Telecom Network IMS	Very High	Open	03/19/2018
Jamming	Telecom Network IMS	Very High	Open	03/19/2018
Interference	Telecom Network IMS	Very High	Open	03/19/2018
TCP Sequence Number Probe	Telecom Network IMS	Low	Open	03/20/2018
TCP ISN Greatest Common Divisor Probe	Telecom Network IMS	Low	Open	03/20/2018
TCP ISN Counter Rate Probe	Telecom Network IMS	Low	Open	03/20/2018
TCP ISN Sequence Predictability Probe	Telecom Network IMS	Low	Open	03/20/2018
TCP Congestion Control Flag Probe	Telecom Network IMS	Low	Open	03/20/2018
TCP Initial Window Size Probe	Telecom Network IMS	Low	Open	03/20/2018
SQL Injection	Telecom Network IMS	High	Open	03/20/2018
Blind SQL Injection	Telecom Network IMS	High	Open	03/20/2018
Persistent Cross Site Scripting - WASC	Telecom Network IMS	High	Open	03/20/2018
Clickjacking	Telecom Network IMS	Very High	Open	03/20/2018