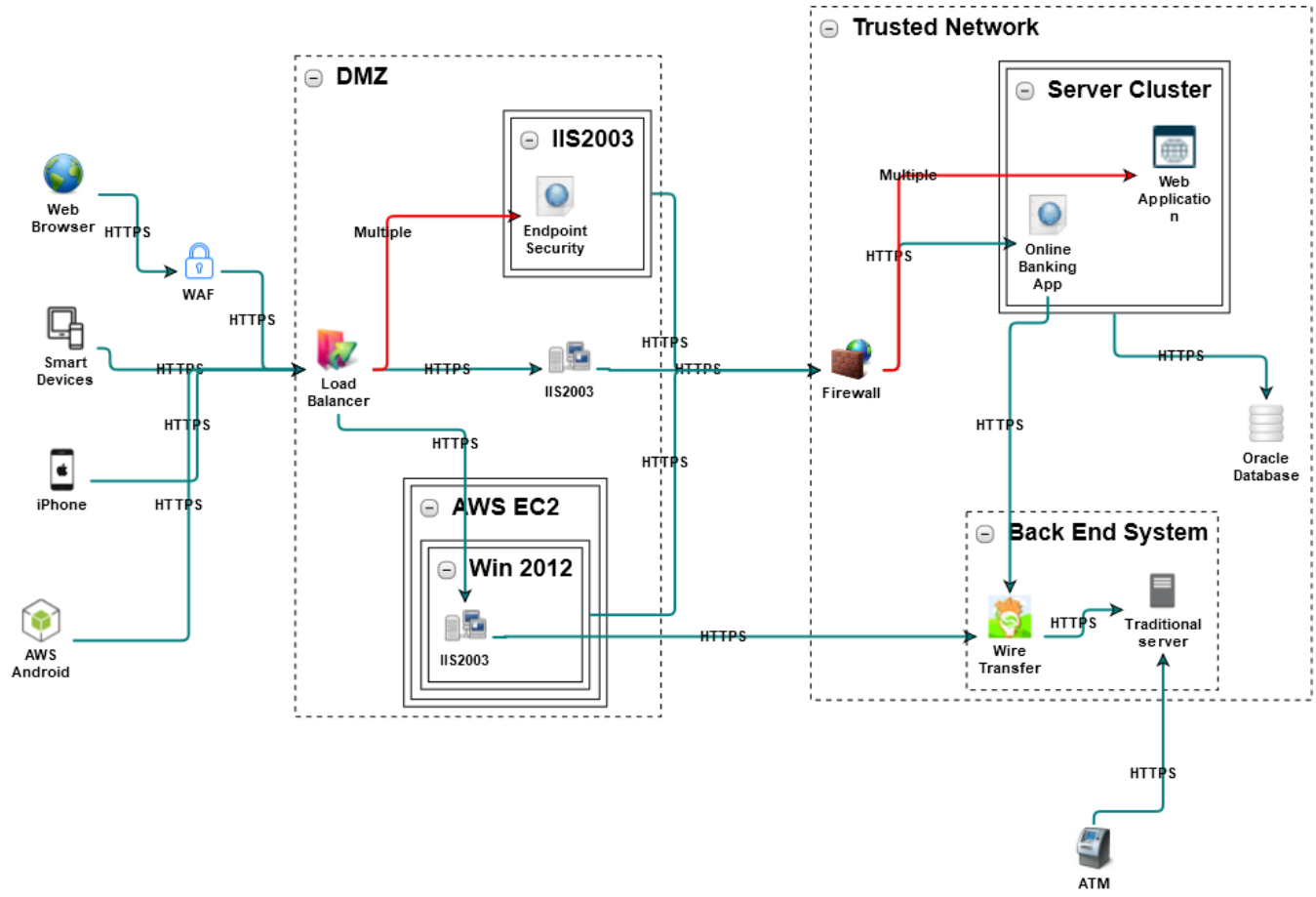
ThreatModeler
Identify • Classify • Prioritize • Mitigate

Banking on-prem Infrastructure - 1

04/10/2018

Threat Model



Description

Threats

Threat	Source	Risk	Status	Date Created
Identity Spoofing - Impersonation	Web Browser	Medium	Open	03/31/2018
Man in the Middle Attack	Web Browser	Very High	Open	03/31/2018
Targeted Malware	Web Browser	Very High	Open	03/31/2018

Account Footprinting	Web Browser	Very High	Open	03/31/2018
Mobile Phone: Camera and or Mic Hijack	Smart Devices	Very Low	Open	03/31/2018
Mobile Phone: Insecure Communications	Smart Devices	Very Low	Open	03/31/2018
Mobile Phone: Session Hijacking	Smart Devices	Very Low	Open	03/31/2018
Mobile Phone: Sensitive Data Leakage	Smart Devices	Very Low	Open	03/31/2018
Mobile Phone: Browser SSL Vulnerability	Smart Devices	Very Low	Open	03/31/2018
Exploiting Incorrectly Configured SSL	HTTPS	Very High	Open	03/31/2018
Overflow Buffers	Win 2012	Very High	Open	03/31/2018
Verify - Insecure Configuration	Win 2012	Very High	Open	03/31/2018
Weak Identity, Credential and Access Management	AWS EC2	Very High	Open	03/31/2018
Denial of Service	AWS EC2	Very High	Open	03/31/2018
Malicious Insiders	AWS EC2	Very High	Open	03/31/2018
Account Hijacking	AWS EC2	Very High	Open	03/31/2018
System and Application Vulnerability	AWS EC2	Very High	Open	03/31/2018
TCP SYN Scan	TCP	Low	Open	03/31/2018
TCP Window Scan	TCP	Low	Open	03/31/2018
TCP RPC Scan	TCP	Low	Open	03/31/2018
TCP Sequence Number Probe	TCP	Low	Open	03/31/2018
TCP ISN Greatest Common Divisor Probe	TCP	Low	Open	03/31/2018
TCP ISN Counter Rate Probe	TCP	Low	Open	03/31/2018
TCP ISN Sequence Predictability Probe	TCP	Low	Open	03/31/2018
TCP Congestion Control Flag Probe	TCP	Low	Open	03/31/2018
TCP Initial Window Size Probe	TCP	Low	Open	03/31/2018
WSDL Scanning	REST API	Very Low	Open	03/31/2018
WS: Injection Flaws	REST API	Very High	Open	03/31/2018
WS: XML Denial of Service	REST API	Very High	Open	03/31/2018
WS: Insecure Communications	REST API	Very High	Open	03/31/2018
WS: Information Leakage	REST API	Very High	Open	03/31/2018
WS: Replay Attack Flaws	REST API	Very	Open	03/31/2018

		High		
WS: Insufficient Authentication	REST API	Very High	Open	03/31/2018
WS: Insecure Configuration	REST API	Very High	Open	03/31/2018
WS: Insufficient Logging	REST API	Very High	Open	03/31/2018
SQL Injection	Oracle Database	High	Open	03/31/2018
Identity Spoofing - Impersonation	ATM	Medium	Open	03/31/2018
Sniffing Attacks	ATM	Medium	Open	03/31/2018
Targeted Malware	ATM	Very High	Open	03/31/2018
Denial of Service	ATM	Very High	Open	03/31/2018
Eavesdropping	ATM	Very High	Open	03/31/2018
Skimming Cards	ATM	Very High	Open	03/31/2018
Skimming Keypads	ATM	Very High	Open	03/31/2018
Spy Cameras	ATM	Very High	Open	03/31/2018
Virtual Channel Theft	ATM	Very High	Open	03/31/2018
Dummy ATMs	ATM	Very High	Open	03/31/2018
Transaction reversal	ATM	Very High	Open	03/31/2018
Currency trapping	ATM	Very High	Open	03/31/2018
Card Trapping	ATM	Very High	Open	03/31/2018
Shoulder Surfing	ATM	High	Open	03/31/2018
Clickjacking	Web Browser	Very High	Open	03/31/2018
HTTP Response Splitting	Web Browser	High	Open	03/31/2018
Cross Site Request Forgery	Web Browser	Very High	Open	03/31/2018
SQL Injection	Web Browser	High	Open	03/31/2018
Blind SQL Injection	Web Browser	High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	Web Browser	High	Open	03/31/2018
Persistent Cross Site Scripting - WASC	Web Browser	High	Open	03/31/2018
Accessing, Intercepting, Modifying HTTP Cookies	Web Browser	High	Open	03/31/2018
Session Hijacking	Web Browser	Very High	Open	03/31/2018
Session Credential Falsification through Forging	Web Browser	Medium	Open	03/31/2018
Reusing Session IDs aka Session Replay	Web Browser	High	Open	03/31/2018

Session Fixation	Web Browser	High	Open	03/31/2018
Dictionary-based Password Attack	Smart Devices	High	Open	03/31/2018
Password Brute Forcing	Smart Devices	High	Open	03/31/2018
Password Recovery Exploitation	Smart Devices	High	Open	03/31/2018
Exploit Common or default Usernames and Passwords	Smart Devices	High	Open	03/31/2018
Dictionary-based Password Attack	Web Browser	High	Open	03/31/2018
Password Brute Forcing	Web Browser	High	Open	03/31/2018
Password Recovery Exploitation	Web Browser	High	Open	03/31/2018
Exploit Common or default Usernames and Passwords	Web Browser	High	Open	03/31/2018
Clickjacking	Smart Devices	Very High	Open	03/31/2018
HTTP Response Splitting	Smart Devices	High	Open	03/31/2018
Cross Site Request Forgery	Smart Devices	Very High	Open	03/31/2018
SQL Injection	Smart Devices	High	Open	03/31/2018
Blind SQL Injection	Smart Devices	High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	Smart Devices	High	Open	03/31/2018
Persistent Cross Site Scripting - WASC	Smart Devices	High	Open	03/31/2018
iOS: Data Storage	iPhone	Very High	Open	03/31/2018
iOS: Weak Server Side Controls	iPhone	Very High	Open	03/31/2018
iOS: Insufficient Transport Layer Protection	iPhone	Very High	Open	03/31/2018
iOS: Client Side Injection	iPhone	Very High	Open	03/31/2018
iOS: Poor Authorization and Authentication	iPhone	Very High	Open	03/31/2018
iOS: Improper Session Handling	iPhone	Very High	Open	03/31/2018
iOS: Security Decisions via Untrusted Inputs	iPhone	Very High	Open	03/31/2018
iOS: Side Channel Data Leakage	iPhone	Very High	Open	03/31/2018
iOS: Broken Encryption	iPhone	Very High	Open	03/31/2018
iOS: Sensitive Information Disclosure	iPhone	Very High	Open	03/31/2018
Probe iOS Screenshots	iPhone	Very High	Open	03/31/2018
Altered Installed BIOS	iPhone	Very High	Open	03/31/2018
Mobile Phone: Camera and or Mic Hijack	AWS Android	Very Low	Open	03/31/2018
Mobile Phone: NFC Vulnerability	AWS Android	Very Low	Open	03/31/2018

Mobile Phone: Insecure Communications	AWS Android	Very Low	Open	03/31/2018
Mobile Phone: Web App Vulnerabilities	AWS Android	Very Low	Open	03/31/2018
Mobile Phone: Session Hijacking	AWS Android	Very Low	Open	03/31/2018
Android: Protocol Vulnerability	AWS Android	Very Low	Open	03/31/2018
Mobile Phone: Sensitive Data Leakage	AWS Android	Very Low	Open	03/31/2018
Mobile Phone: Keylogger	AWS Android	Very Low	Open	03/31/2018
Mobile Phone: Insecure Storage	AWS Android	High	Open	03/31/2018
Mobile Phone: Browser SSL Vulnerability	AWS Android	Very Low	Open	03/31/2018
Targeted Malware	AWS Android	Very High	Open	03/31/2018
Sensitive Data Exposure	Traditional server	Very High	Open	03/31/2018
CVE-2010-1256	IIS2003	Very High	Open	03/31/2018
CVE-2010-1899	IIS2003	Very High	Open	03/31/2018
CVE-2010-2730	IIS2003	Very High	Open	03/31/2018
CVE-2010-3972	IIS2003	Very High	Open	03/31/2018
CVE-2012-2531	IIS2003	Very High	Open	03/31/2018
CVE-2010-1256	IIS2003	Very High	Open	03/31/2018
CVE-2010-1899	IIS2003	Very High	Open	03/31/2018
CVE-2010-2730	IIS2003	Very High	Open	03/31/2018
CVE-2010-3972	IIS2003	Very High	Open	03/31/2018
CVE-2012-2531	IIS2003	Very High	Open	03/31/2018
CVE-2014-1818	Win 2012	Very High	Open	03/31/2018
CVE-2014-1819	Win 2012	Very High	Open	03/31/2018
CVE-2014-1824	Win 2012	Very High	Open	03/31/2018
CVE-2014-1817	Win 2012	Very High	Open	03/31/2018
CVE-2014-1814	Win 2012	Very High	Open	03/31/2018
CVE-2014-1812	Win 2012	Very	Open	03/31/2018

		High		
CVE-2014-1811	Win 2012	Very High	Open	03/31/2018
CVE-2014-1807	Win 2012	Very High	Open	03/31/2018
CVE-2014-1767	Win 2012	Very High	Open	03/31/2018
CVE-2014-0323	Win 2012	Very High	Open	03/31/2018
CVE-2014-0318	Win 2012	Very High	Open	03/31/2018
CVE-2014-0317	Win 2012	Very High	Open	03/31/2018
CVE-2014-0316	Win 2012	Very High	Open	03/31/2018
CVE-2014-0315	Win 2012	Very High	Open	03/31/2018
CVE-2014-0301	Win 2012	Very High	Open	03/31/2018
CVE-2014-0300	Win 2012	Very High	Open	03/31/2018
CVE-2014-0296	Win 2012	Very High	Open	03/31/2018
CVE-2014-0266	Win 2012	Very High	Open	03/31/2018
CVE-2014-0263	Win 2012	Very High	Open	03/31/2018
CVE-2014-0255	Win 2012	Very High	Open	03/31/2018
CVE-2013-5058	Win 2012	Very High	Open	03/31/2018
CVE-2013-3940	Win 2012	Very High	Open	03/31/2018
CVE-2013-3918	Win 2012	Very High	Open	03/31/2018
CVE-2013-3903	Win 2012	Very High	Open	03/31/2018
CVE-2013-3900	Win 2012	Very High	Open	03/31/2018
CVE-2013-3876	Win 2012	Very High	Open	03/31/2018
CVE-2013-3869	Win 2012	Very High	Open	03/31/2018
CVE-2014-2780	Win 2012	Very High	Open	03/31/2018
CVE-2014-2781	Win 2012	Very High	Open	03/31/2018
CVE-2015-0088	Win 2012	Very High	Open	03/31/2018
CVE-2015-0090	Win 2012	Very High	Open	03/31/2018

CVE-2015-0091	Win 2012	Very High	Open	03/31/2018
CVE-2015-0089	Win 2012	Very High	Open	03/31/2018
CVE-2015-0078	Win 2012	Very High	Open	03/31/2018
CVE-2015-0079	Win 2012	Very High	Open	03/31/2018
CVE-2015-0080	Win 2012	Very High	Open	03/31/2018
CVE-2015-0081	Win 2012	Very High	Open	03/31/2018
CVE-2015-0084	Win 2012	Very High	Open	03/31/2018
CVE-2015-0087	Win 2012	Very High	Open	03/31/2018
CVE-2014-4064	Win 2012	Very High	Open	03/31/2018
CVE-2014-4074	Win 2012	Very High	Open	03/31/2018
CVE-2015-0003	Win 2012	Very High	Open	03/31/2018
CVE-2015-0005	Win 2012	Very High	Open	03/31/2018
CVE-2015-0008	Win 2012	Very High	Open	03/31/2018
CVE-2015-0009	Win 2012	Very High	Open	03/31/2018
CVE-2015-0010	Win 2012	Very High	Open	03/31/2018
CVE-2015-0057	Win 2012	Very High	Open	03/31/2018
CVE-2015-0058	Win 2012	Very High	Open	03/31/2018
CVE-2015-0059	Win 2012	Very High	Open	03/31/2018
CVE-2015-0060	Win 2012	Very High	Open	03/31/2018
CVE-2015-0061	Win 2012	Very High	Open	03/31/2018
CVE-2015-0062	Win 2012	Very High	Open	03/31/2018
CVE-2015-0073	Win 2012	Very High	Open	03/31/2018
CVE-2015-0074	Win 2012	Very High	Open	03/31/2018
CVE-2015-0076	Win 2012	Very High	Open	03/31/2018
CVE-2015-0077	Win 2012	Very High	Open	03/31/2018

CVE-2015-0092	Win 2012	Very High	Open	03/31/2018
CVE-2015-0093	Win 2012	Very High	Open	03/31/2018
CVE-2015-1643	Win 2012	Very High	Open	03/31/2018
CVE-2015-1644	Win 2012	Very High	Open	03/31/2018
CVE-2015-1647	Win 2012	Very High	Open	03/31/2018
CVE-2015-0094	Win 2012	Very High	Open	03/31/2018
CVE-2015-0095	Win 2012	Very High	Open	03/31/2018
CVE-2015-0096	Win 2012	Very High	Open	03/31/2018
CVE-2015-1635	Win 2012	Very High	Open	03/31/2018
CVE-2015-1637	Win 2012	Very High	Open	03/31/2018
CVE-2015-1638	Win 2012	Very High	Open	03/31/2018
CVE-2015-1674	Win 2012	Very High	Open	03/31/2018
CVE-2015-1675	Win 2012	Very High	Open	03/31/2018
CVE-2015-1676	Win 2012	Very High	Open	03/31/2018
CVE-2015-1677	Win 2012	Very High	Open	03/31/2018
CVE-2015-1678	Win 2012	Very High	Open	03/31/2018
CVE-2015-1679	Win 2012	Very High	Open	03/31/2018
CVE-2015-1680	Win 2012	Very High	Open	03/31/2018
CVE-2015-1681	Win 2012	Very High	Open	03/31/2018
CVE-2015-1695	Win 2012	Very High	Open	03/31/2018
CVE-2015-1696	Win 2012	Very High	Open	03/31/2018
CVE-2015-1697	Win 2012	Very High	Open	03/31/2018
CVE-2015-1698	Win 2012	Very High	Open	03/31/2018
CVE-2015-1716	Win 2012	Very High	Open	03/31/2018
CVE-2015-1699	Win 2012	Very High	Open	03/31/2018

CVE-2015-1702	Win 2012	Very High	Open	03/31/2018
CVE-2015-1719	Win 2012	Very High	Open	03/31/2018
CVE-2015-1720	Win 2012	Very High	Open	03/31/2018
CVE-2015-1721	Win 2012	Very High	Open	03/31/2018
CVE-2015-1722	Win 2012	Very High	Open	03/31/2018
CVE-2015-1723	Win 2012	Very High	Open	03/31/2018
CVE-2015-1724	Win 2012	Very High	Open	03/31/2018
CVE-2015-1725	Win 2012	Very High	Open	03/31/2018
CVE-2015-1726	Win 2012	Very High	Open	03/31/2018
CVE-2015-1727	Win 2012	Very High	Open	03/31/2018
CVE-2015-2381	Win 2012	Very High	Open	03/31/2018
CVE-2015-1769	Win 2012	Very High	Open	03/31/2018
CVE-2015-2360	Win 2012	Very High	Open	03/31/2018
CVE-2015-2361	Win 2012	Very High	Open	03/31/2018
CVE-2015-2362	Win 2012	Very High	Open	03/31/2018
CVE-2015-2364	Win 2012	Very High	Open	03/31/2018
CVE-2015-2365	Win 2012	Very High	Open	03/31/2018
CVE-2015-2366	Win 2012	Very High	Open	03/31/2018
CVE-2015-2367	Win 2012	Very High	Open	03/31/2018
CVE-2015-2368	Win 2012	Very High	Open	03/31/2018
CVE-2015-2370	Win 2012	Very High	Open	03/31/2018
CVE-2015-2371	Win 2012	Very High	Open	03/31/2018
CVE-2015-2374	Win 2012	Very High	Open	03/31/2018
CVE-2015-2382	Win 2012	Very High	Open	03/31/2018
CVE-2015-2387	Win 2012	Very High	Open	03/31/2018

CVE-2015-1756	Win 2012	Very High	Open	03/31/2018
CVE-2015-2435	Win 2012	Very High	Open	03/31/2018
CVE-2015-2416	Win 2012	Very High	Open	03/31/2018
CVE-2015-2417	Win 2012	Very High	Open	03/31/2018
CVE-2015-2423	Win 2012	Very High	Open	03/31/2018
CVE-2015-2426	Win 2012	Very High	Open	03/31/2018
CVE-2015-2428	Win 2012	Very High	Open	03/31/2018
CVE-2015-2429	Win 2012	Very High	Open	03/31/2018
CVE-2015-2430	Win 2012	Very High	Open	03/31/2018
CVE-2015-2432	Win 2012	Very High	Open	03/31/2018
CVE-2015-2433	Win 2012	Very High	Open	03/31/2018
CVE-2015-2507	Win 2012	Very High	Open	03/31/2018
CVE-2015-2524	Win 2012	Very High	Open	03/31/2018
CVE-2015-2525	Win 2012	Very High	Open	03/31/2018
CVE-2015-2527	Win 2012	Very High	Open	03/31/2018
CVE-2015-2528	Win 2012	Very High	Open	03/31/2018
CVE-2015-2529	Win 2012	Very High	Open	03/31/2018
CVE-2015-2530	Win 2012	Very High	Open	03/31/2018
CVE-2015-2511	Win 2012	Very High	Open	03/31/2018
CVE-2015-2512	Win 2012	Very High	Open	03/31/2018
CVE-2015-2513	Win 2012	Very High	Open	03/31/2018
CVE-2015-2514	Win 2012	Very High	Open	03/31/2018
CVE-2015-2453	Win 2012	Very High	Open	03/31/2018
CVE-2015-2454	Win 2012	Very High	Open	03/31/2018
CVE-2015-2455	Win 2012	Very High	Open	03/31/2018

CVE-2015-2456	Win 2012	Very High	Open	03/31/2018
CVE-2015-2458	Win 2012	Very High	Open	03/31/2018
CVE-2015-2459	Win 2012	Very High	Open	03/31/2018
CVE-2015-2460	Win 2012	Very High	Open	03/31/2018
CVE-2015-2461	Win 2012	Very High	Open	03/31/2018
CVE-2015-2463	Win 2012	Very High	Open	03/31/2018
CVE-2015-2464	Win 2012	Very High	Open	03/31/2018
CVE-2015-2465	Win 2012	Very High	Open	03/31/2018
CVE-2015-2472	Win 2012	Very High	Open	03/31/2018
CVE-2015-2476	Win 2012	Very High	Open	03/31/2018
CVE-2015-2478	Win 2012	Very High	Open	03/31/2018
CVE-2015-2515	Win 2012	Very High	Open	03/31/2018
CVE-2015-2516	Win 2012	Very High	Open	03/31/2018
CVE-2015-2517	Win 2012	Very High	Open	03/31/2018
CVE-2015-2518	Win 2012	Very High	Open	03/31/2018
CVE-2015-2519	Win 2012	Very High	Open	03/31/2018
CVE-2015-2506	Win 2012	Very High	Open	03/31/2018
CVE-2015-2534	Win 2012	Very High	Open	03/31/2018
CVE-2015-2535	Win 2012	Very High	Open	03/31/2018
CVE-2015-2546	Win 2012	Very High	Open	03/31/2018
CVE-2015-2549	Win 2012	Very High	Open	03/31/2018
CVE-2015-2550	Win 2012	Very High	Open	03/31/2018
CVE-2015-2552	Win 2012	Very High	Open	03/31/2018
CVE-2015-2553	Win 2012	Very High	Open	03/31/2018
CVE-2015-2554	Win 2012	Very High	Open	03/31/2018

CVE-2015-6173	Win 2012	Very High	Open	03/31/2018
CVE-2015-6174	Win 2012	Very High	Open	03/31/2018
CVE-2015-6171	Win 2012	Very High	Open	03/31/2018
CVE-2016-0018	Win 2012	Very High	Open	03/31/2018
CVE-2016-0006	Win 2012	Very High	Open	03/31/2018
CVE-2016-0007	Win 2012	Very High	Open	03/31/2018
CVE-2016-0008	Win 2012	Very High	Open	03/31/2018
CVE-2016-0014	Win 2012	Very High	Open	03/31/2018
CVE-2016-0015	Win 2012	Very High	Open	03/31/2018
CVE-2016-0016	Win 2012	Very High	Open	03/31/2018
CVE-2016-0038	Win 2012	Very High	Open	03/31/2018
CVE-2016-0036	Win 2012	Very High	Open	03/31/2018
CVE-2016-0044	Win 2012	Very High	Open	03/31/2018
CVE-2016-0046	Win 2012	Very High	Open	03/31/2018
CVE-2016-0050	Win 2012	Very High	Open	03/31/2018
CVE-2016-0037	Win 2012	Very High	Open	03/31/2018
CVE-2016-0058	Win 2012	Very High	Open	03/31/2018
CVE-2015-6103	Win 2012	Very High	Open	03/31/2018
CVE-2015-6104	Win 2012	Very High	Open	03/31/2018
CVE-2015-6107	Win 2012	Very High	Open	03/31/2018
CVE-2015-6108	Win 2012	Very High	Open	03/31/2018
CVE-2015-6109	Win 2012	Very High	Open	03/31/2018
CVE-2015-6111	Win 2012	Very High	Open	03/31/2018
CVE-2015-6112	Win 2012	Very High	Open	03/31/2018
CVE-2015-6113	Win 2012	Very High	Open	03/31/2018
CVE-2016-3227	Win 2012	Very	Open	03/31/2018

		High		
CVE-2016-3228	Win 2012	Very High	Open	03/31/2018
CVE-2016-3232	Win 2012	Very High	Open	03/31/2018
CVE-2016-3237	Win 2012	Very High	Open	03/31/2018
CVE-2016-3300	Win 2012	Very High	Open	03/31/2018
CVE-2016-3305	Win 2012	Very High	Open	03/31/2018
CVE-2016-3226	Win 2012	Very High	Open	03/31/2018
CVE-2015-6095	Win 2012	Very High	Open	03/31/2018
CVE-2015-6100	Win 2012	Very High	Open	03/31/2018
CVE-2015-6101	Win 2012	Very High	Open	03/31/2018
CVE-2015-6102	Win 2012	Very High	Open	03/31/2018
CVE-2016-3306	Win 2012	Very High	Open	03/31/2018
CVE-2016-3320	Win 2012	Very High	Open	03/31/2018
CVE-2015-6125	Win 2012	Very High	Open	03/31/2018
CVE-2015-6126	Win 2012	Very High	Open	03/31/2018
CVE-2015-6132	Win 2012	Very High	Open	03/31/2018
CVE-2015-6133	Win 2012	Very High	Open	03/31/2018
CVE-2016-3302	Win 2012	Very High	Open	03/31/2018
CVE-2016-3215	Win 2012	Very High	Open	03/31/2018
CVE-2010-1256	IIS2003	Very High	Open	03/31/2018
CVE-2010-1899	IIS2003	Very High	Open	03/31/2018
CVE-2010-2730	IIS2003	Very High	Open	03/31/2018
CVE-2010-3972	IIS2003	Very High	Open	03/31/2018
CVE-2012-2531	IIS2003	Very High	Open	03/31/2018
File Manipulation	Endpoint Security	Medium	Open	03/21/2018
Accessing, Modifying or Executing Executable Files	Endpoint	Very	Open	03/21/2018

	Security	High		
Create files with the same name as files protected with a higher classification	Endpoint Security	Very High	Open	03/21/2018
Force Use of Corrupted Files	Endpoint Security	Medium	Open	03/21/2018
Leveraging or Manipulating Configuration File Search Paths	Endpoint Security	Very High	Open	03/21/2018
User-Controlled Filename	Endpoint Security	High	Open	03/21/2018
Manipulating Web Input to File System Calls	Endpoint Security	Very High	Open	03/21/2018
Bluejacking	Endpoint Security	Very High	Open	03/21/2018
Bluesnarfing	Endpoint Security	Very High	Open	03/21/2018
Bluebugging	Endpoint Security	Very High	Open	03/21/2018
Man in the Middle Attack	Endpoint Security	Very High	Open	03/21/2018
Wi-Fi Jamming	Endpoint Security	High	Open	03/21/2018
WiFi MAC Address Tracking	Endpoint Security	Very High	Open	03/21/2018
WiFi SSID Tracking	Endpoint Security	Very High	Open	03/21/2018
Physical Theft	Endpoint Security	Very High	Open	03/21/2018
Jamming	Endpoint Security	Very High	Open	03/21/2018
File Manipulation	Endpoint Security	Medium	Open	03/21/2018
Accessing, Modifying or Executing Executable Files	Endpoint Security	Very High	Open	03/21/2018
Create files with the same name as files protected with a higher classification	Endpoint Security	Very High	Open	03/21/2018
Manipulating Web Input to File System Calls	Endpoint Security	Very High	Open	03/21/2018
Email Injection	Endpoint Security	Medium	Open	03/21/2018
DNS Cache Poisoning	Endpoint Security	Very High	Open	03/21/2018
Phishing	Endpoint Security	Very High	Open	03/21/2018
Targeted Malware	Endpoint Security	Very High	Open	03/21/2018
SPAM	Endpoint Security	Medium	Open	03/21/2018
Overflow Buffers	Endpoint Security	Very High	Open	03/21/2018
Man in the Middle Attack	Endpoint Security	Very High	Open	03/21/2018

File Manipulation	Endpoint Security	Medium	Open	03/21/2018
Accessing, Modifying or Executing Executable Files	Endpoint Security	Very High	Open	03/21/2018
Create files with the same name as files protected with a higher classification	Endpoint Security	Very High	Open	03/21/2018
Manipulating Web Input to File System Calls	Endpoint Security	Very High	Open	03/21/2018
Identity Spoofing - Impersonation	Endpoint Security	Medium	Open	03/21/2018
Man in the Middle Attack	Endpoint Security	Very High	Open	03/21/2018
Targeted Malware	Endpoint Security	Very High	Open	03/21/2018
Account Footprinting	Endpoint Security	Very High	Open	03/21/2018
Malware Propagation via USB Stick	Endpoint Security	Very High	Open	03/21/2018
DEPRECATED: Malware Propagation via USB U3 Autorun	Endpoint Security	Very High	Open	03/21/2018
DEPRECATED: Malware Propagation via Infected Peripheral Device	Endpoint Security	Very High	Open	03/21/2018
USB Memory Attacks	Endpoint Security	High	Open	03/21/2018
Exploiting Incorrectly Configured SSL	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
IMAP or SMTP Command Injection	Endpoint Security	Medium	Open	03/21/2018
TCP SYN Scan	Endpoint Security	Low	Open	03/21/2018
TCP Window Scan	Endpoint Security	Low	Open	03/21/2018
TCP RPC Scan	Endpoint Security	Low	Open	03/21/2018
TCP Sequence Number Probe	Endpoint Security	Low	Open	03/21/2018
TCP ISN Greatest Common Divisor Probe	Endpoint Security	Low	Open	03/21/2018
TCP ISN Counter Rate Probe	Endpoint Security	Low	Open	03/21/2018
TCP ISN Sequence Predictability Probe	Endpoint Security	Low	Open	03/21/2018
TCP Congestion Control Flag Probe	Endpoint Security	Low	Open	03/21/2018
TCP Initial Window Size Probe	Endpoint Security	Low	Open	03/21/2018

Man in the Middle Attack	Endpoint Security	Very High	Open	03/21/2018
Wi-Fi Jamming	Endpoint Security	High	Open	03/21/2018
WiFi MAC Address Tracking	Endpoint Security	Very High	Open	03/21/2018
WiFi SSID Tracking	Endpoint Security	Very High	Open	03/21/2018
Sensitive Data Exposure	Endpoint Security	Very 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
Email Injection	Endpoint Security	Medium	Open	03/21/2018
IMAP or SMTP Command Injection	Endpoint Security	Medium	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 High	Open	03/21/2018
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
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
Inducing Account Lockout	Online Banking App	Medium	Open	03/31/2018
Man in the browser	Online Banking App	Very High	Open	03/31/2018

Exploiting Incorrectly Configured SSL	Online Banking App	Very High	Open	03/31/2018
Sensitive Data Exposure	Online Banking App	Very High	Open	03/31/2018
Cross Site Request Forgery	Online Banking App	Very High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Sensitive Data Exposure	Online Banking App	Very High	Open	03/31/2018
Clickjacking	Online Banking App	Very High	Open	03/31/2018
HTTP Response Splitting	Online Banking App	High	Open	03/31/2018
Cross Site Request Forgery	Online Banking App	Very High	Open	03/31/2018
SQL Injection	Online Banking App	High	Open	03/31/2018
Blind SQL Injection	Online Banking App	High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Persistent Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Clickjacking	Online Banking App	Very High	Open	03/31/2018
HTTP Response Splitting	Online Banking App	High	Open	03/31/2018
Cross Site Request Forgery	Online Banking App	Very High	Open	03/31/2018
SQL Injection	Online Banking App	High	Open	03/31/2018
Blind SQL Injection	Online Banking App	High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Persistent Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Clickjacking	Online Banking App	Very High	Open	03/31/2018
HTTP Response Splitting	Online Banking App	High	Open	03/31/2018
Cross Site Request Forgery	Online Banking App	Very High	Open	03/31/2018
SQL Injection	Online Banking App	High	Open	03/31/2018
Blind SQL Injection	Online Banking App	High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018

Persistent Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Clickjacking	Online Banking App	Very High	Open	03/31/2018
HTTP Response Splitting	Online Banking App	High	Open	03/31/2018
Cross Site Request Forgery	Online Banking App	Very High	Open	03/31/2018
SQL Injection	Online Banking App	High	Open	03/31/2018
Blind SQL Injection	Online Banking App	High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Persistent Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Clickjacking	Online Banking App	Very High	Open	03/31/2018
HTTP Response Splitting	Online Banking App	High	Open	03/31/2018
Cross Site Request Forgery	Online Banking App	Very High	Open	03/31/2018
SQL Injection	Online Banking App	High	Open	03/31/2018
Blind SQL Injection	Online Banking App	High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Persistent Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Accessing, Intercepting, Modifying HTTP Cookies	Online Banking App	High	Open	03/31/2018
Session Hijacking	Online Banking App	Very High	Open	03/31/2018
Session Credential Falsification through Forging	Online Banking App	Medium	Open	03/31/2018
Reusing Session IDs aka Session Replay	Online Banking App	High	Open	03/31/2018
Session Fixation	Online Banking App	High	Open	03/31/2018
Dictionary-based Password Attack	Online Banking App	High	Open	03/31/2018
Password Brute Forcing	Online Banking App	High	Open	03/31/2018
Password Recovery Exploitation	Online Banking App	High	Open	03/31/2018
Exploit Common or default Usernames and Passwords	Online Banking App	High	Open	03/31/2018
Clickjacking	Online Banking App	Very High	Open	03/31/2018

HTTP Response Splitting	Online Banking App	High	Open	03/31/2018
Cross Site Request Forgery	Online Banking App	Very High	Open	03/31/2018
SQL Injection	Online Banking App	High	Open	03/31/2018
Blind SQL Injection	Online Banking App	High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Persistent Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Dictionary-based Password Attack	Online Banking App	High	Open	03/31/2018
Password Brute Forcing	Online Banking App	High	Open	03/31/2018
Password Recovery Exploitation	Online Banking App	High	Open	03/31/2018
Exploit Common or default Usernames and Passwords	Online Banking App	High	Open	03/31/2018
Sensitive Data Exposure	Online Banking App	Very High	Open	03/31/2018
Clickjacking	Online Banking App	Very High	Open	03/31/2018
HTTP Response Splitting	Online Banking App	High	Open	03/31/2018
Cross Site Request Forgery	Online Banking App	Very High	Open	03/31/2018
SQL Injection	Online Banking App	High	Open	03/31/2018
Blind SQL Injection	Online Banking App	High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Persistent Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Dictionary-based Password Attack	Online Banking App	High	Open	03/31/2018
Password Brute Forcing	Online Banking App	High	Open	03/31/2018
Password Recovery Exploitation	Online Banking App	High	Open	03/31/2018
Exploit Common or default Usernames and Passwords	Online Banking App	High	Open	03/31/2018
Sensitive Data Exposure	Online Banking App	Very High	Open	03/31/2018
Clickjacking	Online Banking App	Very High	Open	03/31/2018
HTTP Response Splitting	Online Banking App	High	Open	03/31/2018

Cross Site Request Forgery	Online Banking App	Very High	Open	03/31/2018
SQL Injection	Online Banking App	High	Open	03/31/2018
Blind SQL Injection	Online Banking App	High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Persistent Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Clickjacking	Online Banking App	Very High	Open	03/31/2018
HTTP Response Splitting	Online Banking App	High	Open	03/31/2018
Cross Site Request Forgery	Online Banking App	Very High	Open	03/31/2018
SQL Injection	Online Banking App	High	Open	03/31/2018
Blind SQL Injection	Online Banking App	High	Open	03/31/2018
Reflected Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018
Persistent Cross Site Scripting - WASC	Online Banking App	High	Open	03/31/2018