ADHOC	ID	Report Vulnerabilities	Category	Total number of articles that cite him
AD13	VUL55	Unauthorized Access	Network	18
AD26	VUL49	Lack of Proper Authentication Mechanisms	Network	15
AD1, AD5	VUL21	Insecure Data Transfer and Storage	Device	13
AD26	VUL27	Lack of Strong Authentication	Device	13
AD15	VUL33	Physical Tampering	Device	13
AD13	VUL37	Weak Access Control	Device	13
AD1, AD5	VUL42	Data Leak or Breach	Network	13
AD11	VUL58	Weak/lack Encryption in Communication	Network	13
AD14	VUL45	Fake/Malicious Node	Network	12
AD12, AD13	VUL4	Insecure Access Management	Application	10
AD11	VUL38	Weak/leak of Encrypt	Device	9
AD3, AD20, AD27	VUL22	Insecure Firmware	Device	8
AD22	VUL51	Lack Secure Communication Protocols	Network	7
AD3, AD12, AD16, AD21	VUL7	Insecure Software	Application	6
AD14	VUL17	Device Spoofing	Device	6
AD10, AD25	VUL31	Obtaining Console Access	Device	6
AD12, AD26	VUL1	Broken Authentication	Application	5
AD1, AD5, AD12	VUL16	Default Configuration	Device	5
AD20	VUL32	Physical Damage	Device	5
AD4	VUL6	Insecure Management of Data	Application	5
AD2	VUL24	Insecure Password	Device	4
AD7	VUL56	Unsecured Network	Network	4
AD2	VUL50	Lack of Strong Password	Network	3
AD8, AD12	VUL5	Insecure Interface Configuration	Application	3
AD11, AD12	VUL12	Weak/lack In-app Encryption	Application	2
AD6, AD12	VUL8	Lack of Active Device Monitoring	Application	1

AD8	VUL39	Insecure physical interface	Device	1
AD3	VUL48	Insecure Update Mechanisms	Network	1
AD18	VUL67	Lack of Technical Support	Peopleware	1
AD19	VUL72	Vendor Security Posture	Peopleware	1

ID	Report Vulnerabilities
AD1	Insecure Data Transfer and Storage
AD2	Weak Passwords
AD3	Insecure Update Mechanisms
AD4	Insufficient Physical Security
AD5	Insufficient Privacy Protection
AD6	Lack of Device Management
AD7	Insecure Network Services
AD8	Insecure Ecosystem Interfaces
AD9	Manipulating the code execution
AD10	Lack of encryption
AD11	Application vulnerabilities
AD12	Incorrect access control
AD13	Intrusion ignorance
AD14	Lack of Trusted Execution Environment
AD15	Outdated software
AD16	Overly large attack surface
AD17	User interaction
AD18	Vendor security posture[CP1]
AD19	Insecure Default Settings
AD20	Insecure or Outdated Components
AD21	TCP/IP Stacks
AD22	Account Lockout
AD23	Insecure 3rd party components
AD24	Obtaining console access
AD25	Two-factor Authentication
AD26	Update Location Writable
AD27	Username Enumeration

Ad-hoc Study x Structured Review

Ad-hoc Literature Review

* White markings highlight vulnerabilities that were not associated with the others in the other study, and for this reason are not included in the "Ad-hoc x Structured" table

ID	Report Vulnerabilities	Category	Total number of articles that cite him
VUL1	Broken Authentication	Application	5
VUL2	Buffer Overflow	Application	7
VUL3	Data Inconsistency	Application	2
VUL4	Insecure Access Management	Application	10
VUL5	Insecure Interface Configuration	Application	3
VUL6	Insecure Management of Data	Application	5
VUL7	Insecure Software	Application	6
VUL8	Lack of Active Device Monitoring	Application	1
VUL9	Low Quality Level Code	Application	1
VUL10	Non-repudiation	Application	4
VUL11	SQL Injections	Application	6
VUL12	Weak/lack In-app Encryption	Application	2
VUL13	Malicious code in-app	Application	3
VUL14	Systems Low-cost	Device	1
VUL15	Channel Voice	Device	2
VUL16	Default Configuration	Device	5
VUL17	Device Spoofing	Device	6
VUL18	Electromagnetic Emanations Leaking	Device	5
VUL19	Energy Restraints	Device	5
VUL20	Heterogeneous Interaction	Device	4
VUL21	Insecure Data Transfer and Storage	Device	13
VUL22	Insecure Firmware	Device	8
VUL23	Insecure Initialization	Device	3
VUL24	Insecure Password	Device	4
VUL25	Insufficient Testing	Device	2
VUL26	Lack of Side Channel Protection	Device	10

VUL27	Lack of Strong Authentication	Device	13
VUL28	Low Computing Power	Device	12
VUL29	Low Data Transmission Range	Device	2
VUL30	Malicious Code Injection	Device	6
VUL31	Obtaining Console Access	Device	6
VUL32	Physical Damage	Device	6
VUL33	Physical Tampering	Device	13
VUL34	Sleep Deprivation	Device	8
VUL35	Tag Cloning	Device	2
VUL36	Unprotected Physical Access	Device	12
VUL37	Weak Access Control	Device	13
VUL38	Weak/leak of Encrypt	Device	9
VUL39	Insecure physical interface	Device	1
VUL40	Channel Interference	Network	11
VUL41	Communication Overhead	Network	1
VUL42	Data Leak or Breach	Network	13
VUL43	Denial of Service	Network	23
VUL44	Eavesdropping	Network	11
VUL45	Fake/Malicious Node	Network	12
VUL46	Heterogeneous Communication	Network	7
VUL47	Insecure Server	Network	3
VUL48	Insecure Update Mechanisms	Network	1
VUL49	Lack of Proper Authentication Mechanisms	Network	15
VUL50	Lack of Strong Password	Network	3
VUL51	Lack Secure Communication Protocols	Network	7
VUL52	Configure network repeatedly	Network	1
VUL53	Single-Point Dependency	Network	1
VUL54	Spoofing Signal	Network	3

VUL55	Unauthorized Access	Network	18
VUL56	Unsecured Network	Network	4
VUL57	Unused Ports Enable	Network	5
VUL58	Weak/lack Encryption in Communication	Network	13
VUL59	Physical properties of the power system	Network	2
VUL60	Wifi De-authentication	Network	1
VUL61	Insecure traffic control	Network	1
VUL62	Centralized architecture	Network	2
VUL63	Botnet	Network	13
VUL64	Access Malicious Link	Peopleware	3
VUL65	Identifying the Product Vendor	Peopleware	1
VUL66	Knowledge the System	Peopleware	3
VUL67	Lack of Technical Support	Peopleware	1
VUL68	Personal and Social Circumstances	Peopleware	5
VUL69	Phishing	Peopleware	10
VUL70	Social Engineering	Peopleware	6
VUL71	Untrusted Device Acquisition	Peopleware	1
VUL72	Vendor Security Posture	Peopleware	1

* White markings highlight vulnerabilities that were not associated with the others in the other study, and for this reason are not included in the "Ad-hoc x Structured" table