Automated Vulnerability-Technique Classification using Semi-Supervised Learning (Appendices)

Ehsan Aghaei[1], Ehab Al-Shaer[1], Waseem Shadid[2], and Xi Niu[2]

[1] Carnegie Mellon University, Pittsburgh PA, USA
{eaghaei, eshaer}@andrew.cmu.edu
[2] University of North Carolina Charlotte NC, USA
{wshadid,xniu2}@uncc.edu

Appendix

1 Vulnerability Types Definitions

#	Vulnerability Type	Connected MITRE ATT&CK Techniques
1	General Improper Access Control	See the Functionality Section
2	Authentication Bypass by Capture-replay	**T1190** (Exploit Public-Facing Application) / **T1040** (Network Sniffing)
3	Improper Restriction of Excessive Authentication Attempts	**T1078** (Valid Accounts) / **T1110.001** (Brute Force: Password Guessing)
4	Overly Restrictive Account Lockout Mechanism	**T1446** (Device Lockout) / **T1531** (Account Access Removal) / **T1110** (Brute Force)
5	Use of Password Hash Instead of Password for Authentication	**T1550.002** (Use Alternate Authentication Material: Pass the Hash)
6	General Credential Management Errors	**T1552** (Unsecured Credentials) / **T1078** (Valid Accounts)
7	Cleartext Transmission of Sensitive Information	**T1552** (Unsecured Credentials) / **T1078** (Valid Accounts) / **T1040** (Network Sniffing)
8	Hard-coded Credentials	**T1078.001** (Default Accounts)
9	Weak Password/Hashing	**T1078** (Valid Accounts) / **T1110** (Brute Force)
10	General Cryptographic Issues	**T1078** (Valid Accounts) / **T1110** (Brute Force) / **T1557** (Man-in-the-Middle) / **T1040** (Network Sniffing)
11	XML External Entity (XXE)	**T1059** (Command and Scripting Interpreter) / **T1005** (Data from Local System) / **T1046** (Network Service Scanning)
12	XML Entity Expansion (XEE)	**T1499.004** (Endpoint Denial of Service: Application or System Exploitation)
14	URL Redirection to Untrusted Site ('Open Redirect')	**T1036** (Masquerading) / **T1566.002** (Phishing: Spearphishing Link)

15	Cross-site Scripting (XSS)	**T1059.007** (Command and Scripting Interpreter: JavaScript/JScript) / **T1557** (Man-in-the-Browser) / -Stored: **T1189** (Drive-by Compromise) -Others **T1204.001** (User Execution: Malicious Link)
16	OS Command Injection	**T1059** (Command and Scripting Interpreter) / **T1133** (External Remote Service)
17	SQL Injection	**T1059** (Command and Scripting Interpreter) / **T1005** (Data from Local System), **T1505.003** (Server Software Component: Web Shell), **T1136** (Create Account) / **T1190** (Exploit Public-Facing Application) / **T1565.001** (Data Manipulation)
18	Code Injection	**T1059** (Command and Scripting Interpreter)
19	Directory Traversal (Relative and Absolute)	See the Functionality Section (File Processing) / See the Functionality Section (File Processing) / **T1202** (Indirect Command Execution)
20	Symlink Attacks	See the Functionality Section (File Processing / See the Functionality Section (File Processing / **T1202** (Indirect Command Execution)
21	Untrusted/ Uncontrolled/ Unquoted Search Path	**T1574** (Hijack Execution Flow)
22	Unrestricted File Upload	**T1505.003** (Server Software Component: Web Shell) / **T1059** (Command and Scripting Interpreter)
23	Deserialization of Untrusted Data	**T1059** (Command and Scripting Interpreter)
24	Infinite Loop	**T1499.004** (Endpoint Denial of Service: Application or System Exploitation)
25	Cross-site Request Forgery (CSRF)	**T1068** (Exploitation for Privilege Escalation) / **T1204.001** (User Execution: Malicious Link)
26	Session Fixation	**T1563** (Remote Service Session Hijacking)
27	Uncontrolled Resource Consumption	**T1499** (Endpoint Denial of Service)
28	Server-Side Request Forgery (SSRF)	**T1090** (Proxy) / **T1135** (Network Discovery) / **T1005** (Data from Local System) / **T1133** (External Remote Service)

Table 1: Vulnerability types mappings to MITRE ATT&CK techniques by MITRE guideline.

2 Functionality to MITRE ATT&CK Technique Mappings

#	Functionality	Connected MITRE ATTACK Techniques
1	Modify Configuration	**T1478** (Install Insecure or Malicious Configuration)
2	Create Account	**T1136** (Create Account) / **T1078** (Valid Accounts)
3	Disable protections	**T1562** (Impair Defenses)
4	Restart/Reboot	**T1529** (System Shutdown/Reboot)
5	Install App	**T1476** (Deliver Malicious App via Other Means)
6	Read from Memory	**T1005** (Data from Local System)
7	Obtain sensitive information: Credentials	**T1552** (Unsecured Credentials)
8	Obtain sensitive information: Other data	**T1005** (Data from Local System)
9	Password Reset	**T1098** (Account Manipulation)
10	Read files	**T1005** (Data from Local System) / **T1003.008** (OS Credential Dumping: /etc/passwd and /etc/shadow) / **T1552.001** (Unsecured Credentials: Credentials in Files)
11	Delete files	**T1485** (Data Destruction) / **T1499.004** (Endpoint Denial of Service: Application or System Exploitation)
12	Create/Upload file	**T1505.003** (Server Software Component: Web Shell) / **T1059** (Command and Scripting Interpreter)
13	Write to existing file	**T1565.001** (Data Manipulation) / **T1059** (Command and Scripting Interpreter) / **T1574** (Hijack Execution Flow) / **T1554** (Compromise Client Software Binary)
14	Change ownership or permissions	**T1222** (File and Directory Permissions Modification)
15	Memory Modification (Memory Buffer Errors, Pointer Issues, Type Errors, etc.)	**T1574** (Hijack Execution Flow), **T1499.004** (Endpoint Denial of Service: Application or System Exploitation)
16	Memory Read (Memory Buffer Errors, Pointer Issues, Type Errors, etc.)	**T1005** (Data from Local System) / **T1499.004** (Endpoint Denial of Service: Application or System Exploitation) / **T1211** (Exploitation for Defense Evasion) / **T1212** (Exploitation for Credential Access)

Table 2: Functionalities' mapping to MITRE ATT&CK techniques by MITRE guideline.

3 Examples of Automated CVEs to Functionalities Classification

z	**Functionality** (f_z)	**Actions** (V_z)	**Object** (O_z)
1	Create Account	add, build, create, establish, generate	account, user account, new user, another user, arbitrary user, ftp user, administrative user, admin user, standard user, root user, admin user, new username, administrator user, administrative user, client
2	Create Or Upload File	add, build, create, dump, upload, generate, transfer, share, transmit	arbitrary posts, content, data, database, directory, drive, existing files, folder, information in the back-end database, insert, log data, log file content, crafted image, crafted photo, data, database, file
3	Delete File	delete, destruction,eliminate, erase, expunge, flush, purge, remove, uninstall, vanish, wipe	arbitrary posts, content, data, database, directories, directory, drive, existing files, files, folder, information in the back-end database, log data, log file
4	Disable Protections	abort, alter, block, corrupt, deactivate. destroy, disable, disconnect, disrupt, downgrade, evade, hinder, impair, interrupt, kill, modify, prevent, reduce, revoke, stop, shut down, terminate, turn off	anti spam, antivirus, antivirus, authentication, authorization, cryptographic protection mechanism, defense, dynamic malware analysis, firewall, guard, intrusion detection, ipsec, protection, secure file copy, security control, security update, shield, signature-based threat detection, ssh, ssl, code signing check, tls, tracking, VPN tunnel
5	Install App	deploy, deliver, install, setup	adware, app, application, crafted request, crafted web request, extension, malicious package, malicious web request, malware, package, phishing, phishing link, place, plugin, program, ransomware, software, spyware, surveillanceware, trojan, virus, widget

6	Modify Configuration	alter, change, compromise, configure, decrypt, edit, elevate, disable, forge, infect, manipulate, modify, poison, rename, replace, restrict, update	management system, administrative setting, configuration, configurator, preference, settings, system management, system property
7	Read From Memory	copy, load, read	memory, buffer, kernel, stack, pointer
8	Read Files	copy, load, observe, open, view, visit	data, database, file, message
9	Memory Read (Memory Buffer Errors, Pointer Issues, Type Errors, etc.)	copy, load, overread, underread, read	active memory, arbitrary kernel memory, arbitrary memory, buffer content, kernel, memory content, memory location, physical memory, process memory, restricted memory, sensitive memory, sensitive memory content, stack memory
10	Memory Modification (Memory Buffer Errors, Pointer Issues, Type Errors, etc.)	change, compromise, configure, forge, infect, manipulate, modify, overwrite, poison, replace, underwrite, update, write	active memory, arbitrary kernel memory, arbitrary memory, buffer content, kernel, memory content, memory location, physical memory, process memory, restricted memory, sensitive memory, sensitive memory content, stack memory
11	Obtain Sensitive Information - Credentials	access, acquire, capture, collect, crack, decrypt, disclose, discover, download, enumerate, expose, extract, find, gain, gather, get, guess, hijack, identify, locate, obtain, reach, retrieve, reveal, scrape, steal, traverse	/shadow, credential, key, /passwd, admin cookie, administrative login access, credentials, cryptographic, passcode, passcodes, password, passwords, plaintext credential, plaintext password, private key, sensitive credential information, session key, user accounts, usernames, user_login, user_pass, username

12	Obtain Sensitive Information - Other Data	access, acquire, capture, collect, disclose, discover, download, enumerate, expose, extract, find, gain, gather, get, guess, hijack, identify, locate, obtain, reach, retrieve, reveal, scrape, steal, traverse	configuration, cookie, database, information, sensitive, session id, string length, token value
13	Password Reset	change, compromise, configure, forge, infect, manipulate, modify, overwrite, poison, replace, update, write	etcpasswd, account, account information, admin, credential, e-mail, email, password, session_key, session key, user_name, user_pass, username
14	Change Ownership or Permissions	change, compromise, configure, decrypt, forge, infect, manipulate, modify, poison, replace, restrict, update	access control list, access to files, delete access, modify access, ownership, read-write permission, read access, read permission, read-write permission, read/write permission, user access, write access, write permission
15	Restart Or Reboot	crash, reboot, restart, shutdown	appliance, camera, computer, crash, device, laptop, modem, phone, process, router, server, service, system
16	Write To Existing File	modify, add, alter, append, change, compromise, edit, forge, insert, manipulate, override, overwrite, poison, rewrite, replace, rewrite, save, store, underwrite, update, write	arbitrary code, arbitrary files, content, database, existing files, source code

Table 3: List of verbs and objects extracted to represent functionality classes

z	**Functionality (f_z)**	**Object (O'_z)**
9	Memory Read (Memory Buffer Errors, Pointer Issues, Type Errors, etc.)	buffer over-read, buffer overread condition, denial of service (heap-based buffer over-read), denial of service (out-of-bounds array access), denial of service (out-of-bounds read and memory corruption), denial of service (out-of-bounds read), out-of-bound read, out-of-bounds access, read past the allocated buffer, reads outside of bounds of heap allocated data
10	Memory Modification (Memory Buffer Errors, Pointer Issues, Type Errors, etc.)	denial of service (out-of-bounds write), out-of-bounds write, overwrite buffers
15	Restart Or Reboot	denial of service (application crash or hang), denial of service (browser crash), denial of service (deadlock), denial of service (device outage), denial of service (device reboot), denial of service (device reload), denial of service (host os crash), denial of service (panic), denial of service (reboot), denial of service (reset), to restart unexpectedly, to reboot

Table 4: List of objects extracted to represent causal links in functionality classes

4 Context-only Evaluation

<table>
<tr><th colspan="3">CVE Description</th></tr>
<tr><th colspan="2">Functionality</th><th>Predicted</th></tr>
<tr><td>1</td><td colspan="2">CVE-2020-5250: In PrestaShop before version 1.7.6.4, when a customer edits their address, they can freely change the id_address in the form, and thus steal someone else's address. It is the same with CustomerForm, you are able to change the id_customer and change all information of all accounts. The problem is patched in version 1.7.6.4.</td></tr>
<tr><td colspan="2">Password Reset
Modify Configuration</td><td>**Password Reset: 7.1**
Modify Configuration: 1.21</td></tr>
<tr><td>2</td><td colspan="2">CVE-2020-15170: apollo-adminservice before version 1.7.1 does not implement access controls. If users expose apollo-adminservice to internet(which is not recommended), there are potential security issues since apollo-adminservice is designed to work in intranet and it doesn't have access control built-in. Malicious hackers may access apollo-adminservice apis directly to access/edit the application's configurations. To fix the potential issue without upgrading, simply follow the advice that do not expose apollo-adminservice to internet.</td></tr>
<tr><td colspan="2">Modify Configuration</td><td>Disable Protections: 8.32
Modify Configuration: 5.18</td></tr>
<tr><td>3</td><td colspan="2">CVE-2020-5253: NetHack before version 3.6.0 allowed malicious use of escaping of characters in the configuration file (usually .nethackrc) which could be exploited. This bug is patched in NetHack 3.6.0.</td></tr>
<tr><td colspan="2">Modify Configuration</td><td>Modify Configuration: 11.27</td></tr>
</table>

<table>
<tr><td>4</td><td colspan="2">CVE-2020-5231: In Opencast before 7.6 and 8.1, users with the role ROLE_COURSE_ADMIN can use the user-utils endpoint to create new users not including the role ROLE_ADMIN. ROLE_COURSE_ADMIN is a non-standard role in Opencast which is referenced neither in the documentation nor in any code (except for tests) but only in the security configuration. From the name – implying an admin for a specific course – users would never expect that this role allows user creation. This issue is fixed in 7.6 and 8.1 which both ship a new default security configuration.</td></tr>
<tr><td colspan="2">Create Account</td><td><b>Create Account: 12.3</b></td></tr>
<tr><td>5</td><td colspan="2">CVE-2013-6129: The install/upgrade.php scripts in vBulletin 4.1 and 5 allow remote attackers to create administrative accounts via the customerid, htmldata[password], htmldata[confirmpassword], and htmldata[email] parameters, as exploited in the wild in October 2013.</td></tr>
<tr><td colspan="2">Create Account</td><td><b>Create Account: 13.84</b></td></tr>
<tr><td>6</td><td colspan="2">CVE-2015-4051: Beckhoff IPC Diagnostics before 1.8 does not properly restrict access to functions in /config, which allows remote attackers to cause a denial of service (reboot or shutdown), create arbitrary users, or possibly have unspecified other impact via a crafted request, as demonstrated by a beckhoff.com:service:cxconfig:1#Write SOAP action to /upnpisapi.</td></tr>
<tr><td colspan="2">Restart Or Reboot
Create Account</td><td><b>Restart Or Reboot: 11.53</b>
<b>Create Account: 5.49</b></td></tr>
<tr><td>7</td><td colspan="2">CVE-2019-3758: RSA Archer, versions prior to 6.6 P2 (6.6.0.2), contain an improper authentication vulnerability. The vulnerability allows sysadmins to create user accounts with insufficient credentials. Unauthenticated attackers could gain unauthorized access to the system using those accounts.</td></tr>
<tr><td colspan="2">Create Account</td><td><b>Create Account: 10.56</b></td></tr>
<tr><td>8</td><td colspan="2">CVE-2019-3798: Cloud Foundry Cloud Controller API Release, versions prior to 1.79.0, contains improper authentication when validating user permissions. A remote authenticated malicious user with the ability to create UAA clients and knowledge of the email of a victim in the foundation may escalate their privileges to that of the victim by creating a client with a name equal to the guid of their victim.</td></tr>
<tr><td colspan="2">Create Account</td><td><b>Create Account: 11.43</b></td></tr>
<tr><td>9</td><td colspan="2">CVE-2019-18581: Dell EMC Data Protection Advisor versions 6.3, 6.4, 6.5, 18.2 versions prior to patch 83, and 19.1 versions prior to patch 71 contain a server missing authorization vulnerability in the REST API. A remote authenticated malicious user with administrative privileges may potentially exploit this vulnerability to alter the application's allowable list of OS commands. This may lead to arbitrary OS command execution as the regular user runs the DPA service on the affected system.</td></tr>
<tr><td colspan="2">Disable protections</td><td><b>Disable Protections: 7.47</b></td></tr>
<tr><td>10</td><td colspan="2">CVE-2018-17908: WebAccess Versions 8.3.2 and prior. During installation, the application installer disables user access control and does not re-enable it after the installation is complete. This could allow an attacker to run elevated arbitrary code.</td></tr>
<tr><td colspan="2">Disable protections</td><td>Install App: 10.31
<b>Disable Protections: 2.81</b></td></tr>
<tr><td>11</td><td colspan="2">CVE-2018-17892: NUUO CMS all versions 3.1 and prior, The application implements a method of user account control that causes standard account security features to not be utilized as intended, which could allow user account compromise and may allow for remote code execution.</td></tr>
</table>

<table>
<tr><td colspan="2">Disable protections</td><td>Obtain Sensitive Information: Credentials: 8.02
<b>Disable Protections: 1.82</b></td></tr>
<tr><td>12</td><td colspan="2">CVE-2018-15397: A vulnerability in the implementation of Traffic Flow Confidentiality (TFC) over IPsec functionality in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to an error that may occur if the affected software renegotiates the encryption key for an IPsec tunnel when certain TFC traffic is in flight. An attacker could exploit this vulnerability by sending a malicious stream of TFC traffic through an established IPsec tunnel on an affected device. A successful exploit could allow the attacker to cause a daemon process on the affected device to crash, which could cause the device to crash and result in a DoS condition.</td></tr>
<tr><td colspan="2">Restart/Reboot</td><td><b>Restart Or Reboot: 14.91</b></td></tr>
<tr><td>13</td><td colspan="2">CVE-2018-15397: A vulnerability in the implementation of Traffic Flow Confidentiality (TFC) over IPsec functionality in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to an error that may occur if the affected software renegotiates the encryption key for an IPsec tunnel when certain TFC traffic is in flight. An attacker could exploit this vulnerability by sending a malicious stream of TFC traffic through an established IPsec tunnel on an affected device. A successful exploit could allow the attacker to cause a daemon process on the affected device to crash, which could cause the device to crash and result in a DoS condition.</td></tr>
<tr><td colspan="2">Restart/Reboot</td><td><b>Restart Or Reboot: 15.05</b></td></tr>
<tr><td>14</td><td colspan="2">CVE-2019-1817: A vulnerability in the web proxy functionality of Cisco AsyncOS Software for Cisco Web Security Appliance could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of HTTP and HTTPS requests. An attacker could exploit this vulnerability by sending a malformed HTTP or HTTPS request to an affected device. An exploit could allow the attacker to cause a restart of the web proxy process, resulting in a temporary DoS condition.</td></tr>
<tr><td colspan="2">Restart/Reboot</td><td><b>Restart Or Reboot: 14.06</b></td></tr>
<tr><td>15</td><td colspan="2">CVE-2020-3312: A vulnerability in the application policy configuration of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to gain unauthorized read access to sensitive data on an affected device. The vulnerability is due to insufficient application identification. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain unauthorized read access to sensitive data.</td></tr>
<tr><td colspan="2">Obtain Sensitive Information: Other Data</td><td><b>Obtain Sensitive Information: Other Data: 8.7588</b></td></tr>
<tr><td>16</td><td colspan="2">CVE-2020-3477: A vulnerability in the CLI parser of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker to access files from the flash: filesystem. The vulnerability is due to insufficient application of restrictions during the execution of a specific command. An attacker could exploit this vulnerability by using a specific command at the command line. A successful exploit could allow the attacker to obtain read-only access to files that are located on the flash: filesystem that otherwise might not have been accessible.</td></tr>
<tr><td colspan="2">Read Files, Obtain Sensitive Information: Other Data</td><td><b>Read Files: 9.47</b>
<b>Obtain Sensitive Information: Other Data: 5.19</b></td></tr>
</table>

17	CVE-2019-15963: A vulnerability in the web-based management interface of Cisco Unified Communications Manager could allow an authenticated, remote attacker to view sensitive information in the web-based management interface of the affected software. The vulnerability is due to insufficient protection of user-supplied input by the web-based management interface of the affected service. An attacker could exploit this vulnerability by accessing the interface and viewing restricted portions of the software configuration. A successful exploit could allow the attacker to gain access to sensitive information or conduct further attacks.
Obtain Sensitive Information: Other Data	**Obtain Sensitive Information: Other Data: 11.4**
18	CVE-2020-11045: In FreeRDP after 1.0 and before 2.0.0, there is an out-of-bound read in in update_read_bitmap_data that allows client memory to be read to an image buffer. The result displayed on screen as colour
Read From Memory	**Read From Memory: 7.54**
19	CVE-2018-7526: In TotalAlert Web Application in BeaconMedaes Scroll Medical Air Systems prior to v4107600010.23, by accessing a specific uniform resource locator (URL) on the webserver, a malicious user may be able to access information in the application without authenticating.
Obtain Sensitive Information: Other Data	**Obtain Sensitive Information: Other Data: 9.89**
20	CVE-2018-5445: A Path Traversal issue was discovered in Advantech WebAccess/SCADA versions prior to V8.2_20170817. An attacker has read access to files within the directory structure of the target device.
Read Files	**Read Files: 13.55**
21	CVE-2018-18990: LCDS Laquis SCADA prior to version 4.1.0.4150 allows a user-supplied path in file operations prior to proper validation. An attacker can leverage this vulnerability to disclose sensitive information under the context of the web server process.
Obtain Sensitive Information: Other Data	**Obtain Sensitive Information: Other Data: 10.04**
22	CVE-2020-16211: Advantech WebAccess HMI Designer, Versions 2.1.9.31 and prior. An out-of-bounds read vulnerability may be exploited by processing specially crafted project files, which may allow an attacker to read information.
Read Files Read From Memory	**Read Files: 7.61** **Read From Memory: 5.15**
23	CVE-2020-11652: An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class allows access to some methods that improperly sanitize paths. These methods allow arbitrary directory access to authenticated users.
Obtain Sensitive Information: Other Data	Obtain Sensitive Information: Credentials: 6.79 **Obtain Sensitive Information: Other Data: 4.93**
24	CVE-2017-16651: Roundcube Webmail before 1.1.10, 1.2.x before 1.2.7, and 1.3.x before 1.3.3 allows unauthorized access to arbitrary files on the host's filesystem, including configuration files, as exploited in the wild in November 2017. The attacker must be able to authenticate at the target system with a valid username/password as the attack requires an active session. The issue is related to file-based attachment plugins and _task=settings_action=upload-display_from=timezone requests.
Read Files	**Read Files: 12.42**

25	CVE-2019-5910: Directory traversal vulnerability in HOUSE GATE App for iOS 1.7.8 and earlier allows remote attackers to read arbitrary files via unspecified vectors.
Read Files	**Read Files: 14.77**
26	CVE-2019-3787: Cloud Foundry UAA, versions prior to 73.0.0, falls back to appending “unknown.org” to a user’s email address when one is not provided and the user name does not contain an @ character. This domain is held by a private company, which leads to attack vectors including password recovery emails sent to a potentially fraudulent address. This would allow the attacker to gain complete control of the user’s account.
Obtain sensitive information: Credentials	**Obtain Sensitive Information: Credentials: 7.69**
27	CVE-2019-3763: The RSA Identity Governance and Lifecycle software and RSA Via Lifecycle and Governance products prior to 7.1.0 P08 contain an information exposure vulnerability. The Office 365 user password may get logged in a plain text format in the Office 365 connector debug log file. An authenticated malicious local user with access to the debug logs may obtain the exposed password to use in further attacks.
Obtain sensitive information: Credentials	**Obtain Sensitive Information: Credentials: 11.86**
28	CVE-2018-17900: Yokogawa STARDOM Controllers FCJ, FCN-100, FCN-RTU, FCN-500, All versions R4.10 and prior, The web application improperly protects credentials which could allow an attacker to obtain credentials for remote access to controllers.
Obtain sensitive information: Credentials	**Obtain Sensitive Information: Credentials: 12.61**
29	CVE-2019-6549: An attacker could retrieve plain-text credentials stored in a XML file on PR100088 Modbus gateway versions prior to Release R02 (or Software Version 1.1.13166) through FTP.
Obtain sensitive information: Credentials	**Obtain Sensitive Information: Credentials: 13.08**
30	CVE-2020-4408: The IBM QRadar Advisor 1.1 through 2.5.2 with Watson App for IBM QRadar SIEM does not adequately mask all passwords during input, which could be obtained by a physical attacker nearby. IBM X-Force ID: 179536.
Obtain sensitive information: Credentials	**Obtain Sensitive Information: Credentials: 8.46**
31	CVE-2019-13922: A vulnerability has been identified in SINEMA Remote Connect Server (All versions V2.0 SP1). An attacker with administrative privileges can obtain the hash of a connected device’s password. The security vulnerability could be exploited by an attacker with network access to the SINEMA Remote Connect Server and administrative privileges. At the time of advisory publication no public exploitation of this security vulnerability was known.
Obtain sensitive information: Credentials	**Obtain Sensitive Information: Credentials: 12.54**
32	CVE-2018-7259: The FSX / P3Dv4 installer 2.0.1.231 for Flight Sim Labs A320-X sends a user’s Google account credentials to http://installLog.flightsimlabs.com/LogHandler3.ashx if a pirated serial number has been entered, which allows remote attackers to obtain sensitive information, e.g., by sniffing the network for cleartext HTTP traffic. This behavior was removed in 2.0.1.232.
Obtain sensitive information: Credentials	**Obtain Sensitive Information: Credentials: 7.17**

33	CVE-2019-15956: A vulnerability in the web management interface of Cisco AsyncOS Software for Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to perform an unauthorized system reset on an affected device. The vulnerability is due to improper authorization controls for a specific URL in the web management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could have a twofold impact: the attacker could either change the administrator password, gaining privileged access, or reset the network configuration details, causing a denial of service (DoS) condition. In both scenarios, manual intervention is required to restore normal operations.
Restart Or Reboot Password Reset	**Restart Or Reboot**: 11.48 Modify Configuration: 3.96 Delete Files: 2.32 Install App: 1.66 **Password Reset: 1.05**
34	CVE-2019-1915: A vulnerability in the web-based interface of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition (SME), Cisco Unified Communications Manager IM and Presence (Unified CM IMamp;P) Service, and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections by the affected software. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could change the password of a targeted user. An attacker could then take unauthorized actions on behalf of the targeted user.
Password Reset	**Password Reset: 9.06**
35	CVE-2019-3775: Cloud Foundry UAA, versions prior to v70.0, allows a user to update their own email address. A remote authenticated user can impersonate a different user by changing their email address to that of a different user.
Password Reset	**Password Reset: 12.08**
36	CVE-2019-3782: Cloud Foundry CredHub CLI, versions prior to 2.2.1, inadvertently writes authentication credentials provided via environment variables to its persistent config file. A local authenticated malicious user with access to the CredHub CLI config file can use these credentials to retrieve and modify credentials stored in CredHub that are authorized to the targeted user.
Password Reset	**Password Reset: 8.88**
37	CVE-2019-3723: Dell EMC OpenManage Server Administrator (OMSA) versions prior to 9.1.0.3 and prior to 9.2.0.4 contain a web parameter tampering vulnerability. A remote unauthenticated attacker could potentially manipulate parameters of web requests to OMSA to create arbitrary files with empty content or delete the contents of any existing file, due to improper input parameter validation
Create Or Upload File Write To Existing File Delete Files	**Create Or Upload File: 9.58** **Write To Existing File: 5.9** **Delete Files: 5.49**
38	CVE-2019-3750: Dell Command Update versions prior to 3.1 contain an Arbitrary File Deletion Vulnerability. A local authenticated malicious user with low privileges potentially could exploit this vulnerability to delete arbitrary files by creating a symlink from the "Temp\IC\ICDebugLog.txt" to any targeted file. This issue occurs because of insecure handling of Temp directory permissions that were set incorrectly.
Delete files	**Delete Files: 13.84**

38	CVE-2020-1163: An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170.
Delete files	**Delete Files: 12.92**
40	CVE-2020-15189: SOY CMS 3.0.2 and earlier is affected by Remote Code Execution (RCE) using Unrestricted File Upload. Cross-Site Scripting(XSS) vulnerability that was used in CVE-2020-15183 can be used to increase impact by redirecting the administrator to access a specially crafted page. This vulnerability is caused by insecure configuration in elFinder. This is fixed in version 3.0.2.328.
Create/Upload file	**Create Or Upload File: 13.11**
41	CVE-2020-5297: In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to upload jpg, jpeg, bmp, png, webp, gif, ico, css, js, woff, woff2, svg, ttf, eot, json, md, less, sass, scss, xml files to any directory of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466).
Create/Upload file	**Create Or Upload File: 15.2911**
42	CVE-2012-6081: Multiple unrestricted file upload vulnerabilities in the (1) twikidraw (action/twikidraw.py) and (2) anywikidraw (action/anywikidraw.py) actions in MoinMoin before 1.9.6 allow remote authenticated users with write permissions to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in an unspecified directory, as exploited in the wild in July 2012.
Create/Upload file	**Create Or Upload File: 14.87**
43	CVE-2011-4106: TimThumb (timthumb.php) before 2.0 does not validate the entire source with the domain white list, which allows remote attackers to upload and execute arbitrary code via a URL containing a white-listed domain in the src parameter, then accessing it via a direct request to the file in the cache directory, as exploited in the wild in August 2011.
Create/Upload file	**Create Or Upload File: 12.71**
44	CVE-2016-3088: The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0 allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.
Create/Upload file	**Create Or Upload File: 14.73**
45	CVE-2020-3476: A vulnerability in the CLI implementation of a specific command of Cisco IOS XE Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying host file system. The vulnerability is due to insufficient validation of the parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of any arbitrary file that resides on the underlying host file system.
Write to existing file	**Write To Existing File: 12.2**
46	CVE-2020-3440: A vulnerability in Cisco Webex Meetings Desktop App for Windows could allow an unauthenticated, remote attacker to overwrite arbitrary files on an end-user system. The vulnerability is due to improper validation of URL parameters that are sent from a website to the affected application. An attacker could exploit this vulnerability by persuading a user to follow a URL to a website that is designed to submit crafted input to the affected application. A successful exploit could allow the attacker to overwrite arbitrary files on the affected system, possibly corrupting or deleting critical system files.
Write to existing file	**Write To Existing File: 12.54**

47	CVE-2019-1836: A vulnerability in the system shell for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an authenticated, local attacker to use symbolic links to overwrite system files. These system files may be sensitive and should not be overwritable by non-root users. The attacker would need valid device credentials. The vulnerability is due to incorrect symbolic link verification of directory paths when they are used in the system shell. An attacker could exploit this vulnerability by authenticating to the device and providing crafted user input to specific symbolic link CLI commands. Successful exploitation could allow the attacker to overwrite system files that should be restricted. This vulnerability has been fixed in software version 14.1(1i).
Write to existing file	**Write To Existing File: 12.6**
48	CVE-2020-3237: A vulnerability in the Cisco Application Framework component of the Cisco IOx application environment could allow an authenticated, local attacker to overwrite arbitrary files in the virtual instance that is running on the affected device. The vulnerability is due to insufficient path restriction enforcement. An attacker could exploit this vulnerability by including a crafted file in an application package. An exploit could allow the attacker to overwrite files.
Write to existing file	**Write To Existing File: 12.79**
49	CVE-2008-4996: init in initramfs-tools 0.92f allows local users to overwrite arbitrary files via a symlink attack on the /tmp/initramfs.debug temporary file.
Write to existing file	**Write To Existing File: 11.4726**
50	CVE-2018-15392: A vulnerability in the DHCP service of Cisco Industrial Network Director could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper handling of DHCP lease requests. An attacker could exploit this vulnerability by sending malicious DHCP lease requests to an affected application. A successful exploit could allow the attacker to cause the DHCP service to terminate, resulting in a DoS condition.
Restart Or Reboot, Memory Read (Memory Errors)	**Restart Or Reboot: 13.34** **Memory Read (Memory Errors): 2.77**
51	CVE-2018-15392: A vulnerability in the DHCP service of Cisco Industrial Network Director could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper handling of DHCP lease requests. An attacker could exploit this vulnerability by sending malicious DHCP lease requests to an affected application. A successful exploit could allow the attacker to cause the DHCP service to terminate, resulting in a DoS condition.
Restart Or Reboot	**Restart Or Reboot: 13.34**
52	CVE-2020-5210: In NetHack before 3.6.5, an invalid argument to the -w command line option can cause a buffer overflow resulting in a crash or remote code execution/privilege escalation. This vulnerability affects systems that have NetHack installed suid/sgid and shared systems that allow users to influence command line options. Users should upgrade to NetHack 3.6.5.
Memory Read (Memory Errors)	**Memory Read (Memory Errors): 6.43**
53	CVE-2020-11019: In FreeRDP less than or equal to 2.0.0, when running with logger set to "WLOG_TRACE", a possible crash of application could occur due to a read of an invalid array index. Data could be printed as string to local terminal. This has been fixed in 2.1.0.
Memory Read (Memory Errors)	**Restart Or Reboot: 11.86** **Memory Read (Memory Errors): 2.35**

54	CVE-2020-15137: All versions of HoRNDIS are affected by an integer overflow in the RNDIS packet parsing routines. A malicious USB device can trigger disclosure of unrelated kernel memory to userspace applications on the host, or can cause the kernel to crash. Kernel memory disclosure is especially likely on 32-bit kernels; 64-bit kernels are more likely to crash on attempted exploitation. It is not believed that kernel memory corruption is possible, or that unattended kernel memory disclosure without the collaboration of a userspace program running on the host is possible. The vulnerability is in `HoRNDIS::receivePacket`. `msg_len`, `data_ofs`, and `data_len` can be controlled by an attached USB device, and a negative value of `data_ofs` can bypass the check for `(data_ofs + data_len + 8) msg_len`, and subsequently can cause a wild pointer copy in the `mbuf_copyback` call. The software is not maintained and no patches are planned. Users of multi-tenant systems with HoRNDIS installed should only connect trusted USB devices to their system.
Memory Read (Memory Errors)	**Memory Read (Memory Errors): 7.3**
55	CVE-2020-4068: In APNSwift 1.0.0, calling APNSwiftSigner.sign(digest:) is likely to result in a heap buffer overflow. This has been fixed in 1.0.1.
Memory Read (Memory Errors)	**Memory Read (Memory Errors): 9.26**
56	CVE-2020-15199: In Tensorflow before version 2.3.1, the `RaggedCountSparseOutput` does not validate that the input arguments form a valid ragged tensor. In particular, there is no validation that the `splits` tensor has the minimum required number of elements. Code uses this quantity to initialize a different data structure. Since `BatchedMap` is equivalent to a vector, it needs to have at least one element to not be `nullptr`. If user passes a `splits` tensor that is empty or has exactly one element, we get a `SIGABRT` signal raised by the operating system.
Memory Read (Memory Errors)	Restart Or Reboot: 4.26 **Memory Read (Memory Errors): 3.88**
57	CVE-2020-11068: In LoRaMac-node before 4.4.4, a reception buffer overflow can happen due to the received buffer size not being checked. This has been fixed in 4.4.4
Memory Read (Memory Errors)	**Memory Read (Memory Errors): 9.9**
58	CVE-2020-8649: There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the vgacon_invert_region function in drivers/video/console/vgacon.c.
Memory Read (Memory Errors)	**Memory Read (Memory Errors): 9.44**
59	CVE-2020-12652: The __mptctl_ioctl function in drivers/message/fusion/mptctl.c in the Linux kernel before 5.4.14 allows local users to hold an incorrect lock during the ioctl operation and trigger a race condition, i.e., a "double fetch" vulnerability, aka CID-28d76df18f0a. NOTE: the vendor states "The security impact of this bug is not as bad as it could have been because these operations are all privileged and root already has enormous destructive power."
Memory Read (Memory Errors)	**Memory Read (Memory Errors): 8.22**
60	CVE-2019-12660: A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker to write values to the underlying memory of an affected device. The vulnerability is due to improper input validation and authorization of specific commands that a user can execute within the CLI. An attacker could exploit this vulnerability by authenticating to an affected device and issuing a specific set of commands. A successful exploit could allow the attacker to modify the configuration of the device to cause it to be non-secure and abnormally functioning.
Memory Modification (Memory Errors)	**Memory Modification (Memory Errors): 10.97**

61	CVE-2019-13522: An attacker could use a specially crafted project file to corrupt the memory and execute code under the privileges of the EZ PLC Editor Versions 1.8.41 and prior.
Memory Modification (Memory Errors)	**Memory Modification (Memory Errors): 11.15**
62	CVE-2018-10620: AVEVA InduSoft Web Studio v8.1 and v8.1SP1, and InTouch Machine Edition v2017 8.1 and v2017 8.1 SP1 a remote user could send a carefully crafted packet to exploit a stack-based buffer overflow vulnerability during tag, alarm, or event related actions such as read and write, with potential for code to be executed.
Memory Read (Memory Errors), Memory Modification (Memory Errors)	**Memory Read (Memory Errors): 4.84** **Memory Modification (Memory Errors): 1.84**
63	CVE-2019-12660: A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker to write values to the underlying memory of an affected device. The vulnerability is due to improper input validation and authorization of specific commands that a user can execute within the CLI. An attacker could exploit this vulnerability by authenticating to an affected device and issuing a specific set of commands. A successful exploit could allow the attacker to modify the configuration of the device to cause it to be non-secure and abnormally functioning.
Memory Modification (Memory Errors), Disable Protections	**Memory Modification (Memory Errors): 10.97** **Disable Protections: 2.81**
64	CVE-2018-15376: A vulnerability in the embedded test subsystem of Cisco IOS Software for Cisco 800 Series Industrial Integrated Services Routers could allow an authenticated, local attacker to write arbitrary values to arbitrary locations in the memory space of an affected device. The vulnerability is due to the presence of certain test commands that were intended to be available only in internal development builds of the affected software. An attacker could exploit this vulnerability by using these commands on an affected device. A successful exploit could allow the attacker to write arbitrary values to arbitrary locations in the memory space of the affected device.
Memory Modification (Memory Errors)	**Memory Modification (Memory Errors): 11.77**
65	CVE-2019-1052: A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'.
Memory Read (Memory Errors)	**Memory Read (Memory Errors): 10.11**
66	CVE-2020-3309: A vulnerability in Cisco Firepower Device Manager (FDM) On-Box software could allow an authenticated, remote attacker to overwrite arbitrary files on the underlying operating system of an affected device. The vulnerability is due to improper input validation. An attacker could exploit this vulnerability by uploading a malicious file to an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on as well as modify the underlying operating system of an affected device.
Write To Existing File	**Write To Existing File: 10.73**

Table 5: The evaluation of classifying 66 CVE into one or more functionalities based on only the description without considering the second input. The table shows the top K prediction for each CVE description where K equals to the total number of predictions until all the correct classes are predicted. The correct predictions are depicted by bold font.