Vulnerability report for 192.168.56.103

Student: Markus Ijäs

This report contains all vulnerabilities with CVSS score of 5.0 or more found in the target machine (192.168.56.103) provided in the Information Security course at TUAS.

The work was started by mapping the vulnerabilities with `nmap -sV --script vulners 192.168.56.103` since this is the Debian-equivalent for the generic vulnerability discovery script `nmap-vulners`.

All descriptions are taken from the respective Vulners.com page (link provided right after each description). All Common Weakness Enumeration (CWE) descriptions are presented at the bottom of this document and are taken from mitre.org pages linked right after each description.

I'm also not fully ok with scraping those websites for massive amounts of data (it's particularly not ok if this report would be presented to a real customer. That would require me to properly license the data provided).

Found vulnerabilities (CVEs)

ProFTPD 1.3.5

CVE-2015-3306 (CVSS 10.0, CWE-284)

The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.

https://vulners.com/cve/CVE-2015-3306

CVE-2019-19272 (CVSS 5.0, CWE-476)

An issue was discovered in tls_verify_crl in ProFTPD before 1.3.6. Direct dereference of a NULL pointer (a variable initialized to NULL) leads to a crash when validating the certificate of a client connecting to the server in a TLS client/server mutual-authentication setup.

https://vulners.com/cve/CVE-2019-19272

CVE-2019-19271 (CVSS 5.0, CWE-295)

An issue was discovered in tls_verify_crl in ProFTPD before 1.3.6. A wrong iteration variable, used when checking a client certificate against CRL entries (installed by a system administrator), can cause some CRL entries to be ignored, and can allow clients whose certificates have been revoked to proceed with a connection to the server.

https://vulners.com/cve/CVE-2019-19271

CVE-2019-19270 (CVSS 5.0, CWE-295)

An issue was discovered in tls_verify_crl in ProFTPD through 1.3.6b. Failure to check for the appropriate field of a CRL entry (checking twice for subject, rather than once for subject and once for issuer) prevents some valid CRLs from being taken into account, and can allow clients whose certificates have been revoked to proceed with a connection to the server.

https://vulners.com/cve/CVE-2019-19270

CVE-2019-18217 (CVSS 5.0, CWE-835)

ProFTPD before 1.3.6b and 1.3.7rc before 1.3.7rc2 allows remote unauthenticated denial-of-service due to incorrect handling of overly long commands because main.c in a child process enters an infinite loop.

https://vulners.com/cve/CVE-2019-18217

CVE-2016-3125 (CVSS 5.0, CWE-310, CWE-254)

The mod_tls module in ProFTPD before 1.3.5b and 1.3.6 before 1.3.6rc2 does not properly handle the TLSDHParamFile directive, which might cause a weaker than intended Diffie-Hellman (DH) key to be used and consequently allow attackers to have unspecified impact via unknown vectors.

https://vulners.com/cve/CVE-2016-3125

CVE-2013-4359 (CVSS 5.0, CWE-189)

Integer overflow in kbdint.c in mod_sftp in ProFTPD 1.3.4d and 1.3.5r3 allows remote attackers to cause a denial of service (memory consumption) via a large response count value in an authentication request, which triggers a large memory allocation.

https://vulners.com/cve/CVE-2013-4359

OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)

CVE-2015-5600 (CVSS 8.5, CWE-264)

The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.

https://vulners.com/cve/CVE-2015-5600

CVE-2015-6564 (CVSS 6.9, CWE-264)

Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.

https://vulners.com/cve/CVE-2015-6564

CVE-2018-15919 (CVSS 5.0, CWE-200)

Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'

https://vulners.com/cve/CVE-2018-15919

Apache/2.4.7 (Ubuntu)

CVE-2021-39275 (CVSS 7.5, CWE-120)

ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

https://vulners.com/cve/CVE-2021-39275

CVE-2021-26691 (CVSS 7.5, CWE-787)

In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

https://vulners.com/cve/CVE-2021-26691

CVE-2017-7679 (CVSS 7.5, CWE-119)

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

https://vulners.com/cve/CVE-2017-7679

CVE-2017-3167 (CVSS 7.5, CWE-287)

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

https://vulners.com/cve/CVE-2017-3167

CVE-2021-40438 (CVSS 6.8, CWE-918)

A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

https://vulners.com/cve/CVE-2021-40438

CVE-2020-35452 (CVSS 6.8, CWE-787)

Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

https://vulners.com/cve/CVE-2020-35452

CVE-2018-1312 (CVSS 6.8, CWE-287)

In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

https://vulners.com/cve/CVE-2018-1312

CVE-2017-15715 (CVSS 6.8, CWE-20)

In Apache httpd 2.4.0 to 2.4.29, the expression specified in could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

https://vulners.com/cve/CVE-2017-15715

CVE-2014-0226 (CVSS 6.8, CWE-362)

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

https://vulners.com/cve/CVE-2014-0226

CVE-2017-9788 (CVSS 6.4, CWE-200, CWE-20)

In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

https://vulners.com/cve/CVE-2017-9788

CVE-2019-0217 (CVSS 6.0, CWE-362)

In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

https://vulners.com/cve/CVE-2019-0217

CVE-2020-1927 (CVSS 5.8, CWE-601)

In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

https://vulners.com/cve/CVE-2020-1927

CVE-2019-10098 (CVSS 5.8, CWE-601)

In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

https://vulners.com/cve/CVE-2019-10098

CVE-2016-5387 (CVSS 5.1, CWE-284)

The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

https://vulners.com/cve/CVE-2016-5387

CVE-2021-34798 (CVSS 5.0, CWE-476)

Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

https://vulners.com/cve/CVE-2021-34798

CVE-2021-26690 (CVSS 5.0, CWE-476)

Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

https://vulners.com/cve/CVE-2021-26690

CVE-2020-1934 (CVSS 5.0, CWE-908)

In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

https://vulners.com/cve/CVE-2020-1934

CVE-2019-17567 (CVSS 5.0, CWE-444)

Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

https://vulners.com/cve/CVE-2019-17567

CVE-2019-0220 (CVSS 5.0, CWE-706)

A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

https://vulners.com/cve/CVE-2019-0220

CVE-2018-17199 (CVSS 5.0, CWE-384)

In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

https://vulners.com/cve/CVE-2018-17199

CVE-2018-1303 (CVSS 5.0, CWE-125)

A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

https://vulners.com/cve/CVE-2018-1303

CVE-2017-9798 (CVSS 5.0, CWE-416)

Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

https://vulners.com/cve/CVE-2017-9798

CVE-2017-15710 (CVSS 5.0, CWE-787)

In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

https://vulners.com/cve/CVE-2017-15710

CVE-2016-8743 (CVSS 5.0, CWE-19)

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

https://vulners.com/cve/CVE-2016-8743

CVE-2016-2161 (CVSS 5.0, CWE-20)

In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

https://vulners.com/cve/CVE-2016-2161

CVE-2016-0736 (CVSS 5.0, CWE-310)

In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

https://vulners.com/cve/CVE-2016-0736

CVE-2015-3183 (CVSS 5.0, CWE-20, CWE-17)

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

https://vulners.com/cve/CVE-2015-3183

CVE-2015-0228 (CVSS 5.0, CWE-20)

The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

https://vulners.com/cve/CVE-2015-0228

CVE-2014-0231 (CVSS 5.0, CWE-399)

The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

https://vulners.com/cve/CVE-2014-0231

CVE-2014-0098 (CVSS 5.0, CWE-20)

The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

https://vulners.com/cve/CVE-2014-0098

CVE-2013-6438 (CVSS 5.0, CWE-20)

The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

https://vulners.com/cve/CVE-2013-6438

CUPS/1.7 IPP/2.1

CVE-2012-5519 (CVSS 7.2, CWE-264)

CUPS 1.4.4, when running in certain Linux distributions such as Debian GNU/Linux, stores the web interface administrator key in /var/run/cups/certs/0 using certain permissions, which allows local users in the lpadmin group to read or write arbitrary files as root by leveraging the web interface.

https://vulners.com/cve/CVE-2012-5519

CVE-2014-5031 (CVSS 5.0, CWE-164)

The web interface in CUPS before 2.0 does not check that files have world-readable permissions, which allows remote attackers to obtains sensitive information via unspecified vectors.

https://vulners.com/cve/CVE-2014-5031

WEBrick/1.3.1 (Ruby/2.3.7/2018-03-28)

CVE-2018-8780 (CVSS 7.5, CWE-22)

In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, the Dir.open, Dir.new, Dir.entries and Dir.empty? methods do not check NULL characters. When using the corresponding method, unintentional directory traversal may be performed.

https://vulners.com/cve/CVE-2018-8780

CVE-2018-16395 (CVSS 7.5)

An issue was discovered in the OpenSSL library in Ruby before 2.3.8, 2.4.x before 2.4.5, 2.5.x before 2.5.2, and 2.6.x before 2.6.0-preview3. When two OpenSSL::X509::Name objects are compared using ==, depending on the ordering, non-equal objects may return true. When the first argument is one character longer than the second, or the second argument contains a character that is one less than a character in the same position of the first argument, the result of == will be true. This could be leveraged to create an illegitimate certificate that may be accepted as legitimate and then used in signing or encryption operations.

https://vulners.com/cve/CVE-2018-16395

CVE-2018-16396 (CVSS 6.8)

An issue was discovered in Ruby before 2.3.8, 2.4.x before 2.4.5, 2.5.x before 2.5.2, and 2.6.x before 2.6.0-preview3. It does not taint strings that result from unpacking tainted strings with some formats.

https://vulners.com/cve/CVE-2018-16396

CVE-2018-8779 (CVSS 5.0, CWE-20)

In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, the UNIXServer.open and UNIXSocket.open methods are not checked for null characters. It may be connected to an unintended socket.

https://vulners.com/cve/CVE-2018-8779

CVE-2018-8778 (CVSS 5.0, CWE-134)

In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, an attacker controlling the unpacking format (similar to format string vulnerabilities) can trigger a buffer under-read in the String#unpack method, resulting in a massive and controlled information disclosure.

https://vulners.com/cve/CVE-2018-8778

CVE-2018-8777 (CVSS 5.0, CWE-400)

In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, an attacker can pass a large HTTP request with a crafted header to WEBrick server or a crafted body to WEBrick server/handler and cause a denial of service (memory consumption).

https://vulners.com/cve/CVE-2018-8777

CVE-2018-6914 (CVSS 5.0, CWE-22)

Directory traversal vulnerability in the Dir.mktmpdir method in the tmpdir library in Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1 might allow attackers to create arbitrary directories or files via a ... (dot dot) in the prefix argument.

https://vulners.com/cve/CVE-2018-6914

CWE Descriptions

CWE-284

The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

https://cwe.mitre.org/data/definitions/284.html

CWE-264

Weaknesses in this category are related to the management of permissions, privileges, and other security features that are used to perform access control.

https://cwe.mitre.org/data/definitions/264.html

CWE-476

A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit.

https://cwe.mitre.org/data/definitions/476.html

CWE-295

The software does not validate, or incorrectly validates, a certificate.

https://cwe.mitre.org/data/definitions/295.html

CWE-835

The program contains an iteration or loop with an exit condition that cannot be reached, i.e., an infinite loop.

https://cwe.mitre.org/data/definitions/835.html

CWE-310

Weaknesses in this category are related to the design and implementation of data confidentiality and integrity. Frequently these deal with the use of encoding

techniques, encryption libraries, and hashing algorithms. The weaknesses in this category could lead to a degradation of the quality data if they are not addressed.

https://cwe.mitre.org/data/definitions/310.html

CWE-254

Software security is not security software. Here we're concerned with topics like authentication, access control, confidentiality, cryptography, and privilege management.

https://cwe.mitre.org/data/definitions/254.html

CWE-189

Weaknesses in this category are related to improper calculation or conversion of numbers.

https://cwe.mitre.org/data/definitions/189.html

CWE-200

The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

https://cwe.mitre.org/data/definitions/200.html

CWE-120

The program copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow.

https://cwe.mitre.org/data/definitions/120.html

CWE-787

The software writes data past the end, or before the beginning, of the intended buffer.

https://cwe.mitre.org/data/definitions/787.html

CWE-119

The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer.

https://cwe.mitre.org/data/definitions/119.html

CWE-287

When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct.

https://cwe.mitre.org/data/definitions/287.html

CWE-918

The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

https://cwe.mitre.org/data/definitions/918.html

CWE-20

The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

https://cwe.mitre.org/data/definitions/20.html

CWE-362

The program contains a code sequence that can run concurrently with other code, and the code sequence requires temporary, exclusive access to a shared resource, but a timing window exists in which the shared resource can be modified by another code sequence that is operating concurrently.

https://cwe.mitre.org/data/definitions/362.html

CWE-601

A web application accepts a user-controlled input that specifies a link to an external site, and uses that link in a Redirect. This simplifies phishing attacks.

https://cwe.mitre.org/data/definitions/601.html

CWE-908

The software uses or accesses a resource that has not been initialized.

https://cwe.mitre.org/data/definitions/908.html

CWE-444

When malformed or abnormal HTTP requests are interpreted by one or more entities in the data flow between the user and the web server, such as a proxy or

firewall, they can be interpreted inconsistently, allowing the attacker to "smuggle" a request to one device without the other device being aware of it.

https://cwe.mitre.org/data/definitions/444.html

CWE-706

The software uses a name or reference to access a resource, but the name/reference resolves to a resource that is outside of the intended control sphere.

https://cwe.mitre.org/data/definitions/706.html

CWE-384

Authenticating a user, or otherwise establishing a new user session, without invalidating any existing session identifier gives an attacker the opportunity to steal authenticated sessions.

https://cwe.mitre.org/data/definitions/384.html

CWE-125

The software reads data past the end, or before the beginning, of the intended buffer.

https://cwe.mitre.org/data/definitions/125.html

CWE-416

Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code.

https://cwe.mitre.org/data/definitions/416.html

CWE-19

Weaknesses in this category are typically found in functionality that processes data. Data processing is the manipulation of input to retrieve or save information.

https://cwe.mitre.org/data/definitions/19.html

CWE-17

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

https://cwe.mitre.org/data/definitions/17.html

CWE-399

Weaknesses in this category are related to improper management of system resources.

https://cwe.mitre.org/data/definitions/399.html

CWE-22

The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

https://cwe.mitre.org/data/definitions/22.html

CWE-134

The software uses a function that accepts a format string as an argument, but the format string originates from an external source.

https://cwe.mitre.org/data/definitions/134.html

CWE-400

The software does not properly control the allocation and maintenance of a limited resource, thereby enabling an actor to influence the amount of resources consumed, eventually leading to the exhaustion of available resources.

https://cwe.mitre.org/data/definitions/400.html