SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 02 June 2021

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-32637	Authelia is a a single sign-on multi-factor portal for web apps. This affects uses who are using nginx ngx_http_auth_request_module with Authelia, it allows a malicious individual who crafts a malformed HTTP request to bypass the authentication mechanism. It additionally could theoretically affect other proxy servers, but all of the ones we officially support except nginx do not allow malformed URI paths. The problem is rectified entirely in v4.29.3. As this patch is relatively straightforward we can back port this to any version upon request. Alternatively we are supplying a git patch to 4.25.1 which should be relatively straightforward to apply to any version, the git patches for specific versions can be found in the references. The most relevant workaround is upgrading. You can also add a block which fails requests that contains a malformed URI in the internal location block.	10.0	More Details
CVE-2020-4561	IBM Cognos Analytics 11.0 and 11.1 DQM API allows submitting of all control requests in unauthenticated sessions. This allows a remote attacker who can access a valid CA endpoint to read and write files to the Cognos Analytics system. IBM X-Force ID: 183903.	10.0	More Details
CVE-2021-22160	If Apache Pulsar is configured to authenticate clients using tokens based on JSON Web Tokens (JWT), the signature of the token is not validated if the algorithm of the presented token is set to "none". This allows an attacker to connect to Pulsar instances as any user (incl. admins).	9.8	More Details
CVE-2021-31703	Frontier ichris through 5.18 allows users to upload malicious executable files that might later be downloaded and run by any client user.	9.8	More Details
CVE-2021-20236	A flaw was found in the ZeroMQ server in versions before 4.3.3. This flaw allows a malicious client to cause a stack buffer overflow on the server by sending crafted topic subscription requests and then unsubscribing. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	9.8	More Details
CVE-2020-15782	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0), SINAMICS PERFECT HARMONY GH180 Drives (Drives manufactured before 2021-08-13), SINUMERIK MC (All versions < V6.15), SINUMERIK ONE (All versions < V6.15). Affected devices are vulnerable to a memory protection bypass through a specific operation. A remote unauthenticated attacker with network access to port 102/tcp could potentially write arbitrary data and code to protected memory areas or read sensitive data to launch further attacks.	9.8	More Details
CVE-2021-22519	Execute arbitrary code vulnerability in Micro Focus SiteScope product, affecting versions 11.40,11.41 , 2018.05(11.50), 2018.08(11.51), 2018.11(11.60), 2019.02(11.70), 2019.05(11.80), 2019.08(11.90), 2019.11(11.91), 2020.05(11.92), 2020.10(11.93). The vulnerability could allow remote attackers to execute arbitrary code on affected installations of SiteScope.	9.8	More Details
CVE-2021-32619	Deno is a runtime for JavaScript and TypeScript that uses V8 and is built in Rust. In Deno versions 1.5.0 to 1.10.1, modules that are dynamically imported through `import()` or `new Worker` might have been able to bypass network and file system permission checks when statically importing other modules. The vulnerability has been patched in Deno release 1.10.2.	9.8	More Details
CVE-2021-30461	A remote code execution issue was discovered in the web UI of VoIPmonitor before 24.61. When the recheck option is used, the user-supplied SPOOLDIR value (which might contain PHP code) is injected into config/configuration.php.	9.8	More Details
CVE-2021-33564	An argument injection vulnerability in the Dragonfly gem before 1.4.0 for Ruby allows remote attackers to read and write to arbitrary files via a crafted URL when the verify_url option is disabled. This may lead to code execution. The problem occurs because the generate and process features mishandle use of the ImageMagick convert utility.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21985	The vSphere Client (HTML5) contains a remote code execution vulnerability due to lack of input validation in the Virtual SAN Health Check plug-in which is enabled by default in vCenter Server. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server.	9.8	More Details
CVE-2021-33790	The RebornCore library before 4.7.3 allows remote code execution because it deserializes untrusted data in ObjectInputStream.readObject as part of reborncore.common.network.ExtendedPacketBuffer. An attacker can instantiate any class on the classpath with any data. A class usable for exploitation might or might not be present, depending on what Minecraft modifications are installed.	9.8	More Details
CVE-2020-10666	The restapps (aka Rest Phone apps) module for Sangoma FreePBX and PBXact 13, 14, and 15 through 15.0.19.2 allows remote code execution via a URL variable to an AMI command.	9.8	More Details
CVE-2021-24321	The Bello - Directory & Listing WordPress theme before 1.6.0 did not sanitise the bt_bb_listing_field_price_range_to, bt_bb_listing_field_now_open, bt_bb_listing_field_my_lng, listing_list_view and bt_bb_listing_field_my_lat parameters before using them in a SQL statement, leading to SQL Injection issues	9.8	More Details
CVE-2021-25641	Each Apache Dubbo server will set a serialization id to tell the clients which serialization protocol it is working on. But for Dubbo versions before 2.7.8 or 2.6.9, an attacker can choose which serialization id the Provider will use by tampering with the byte preamble flags, aka, not following the server's instruction. This means that if a weak deserializer such as the Kryo and FST are somehow in code scope (e.g. if Kryo is somehow a part of a dependency), a remote unauthenticated attacker can tell the Provider to use the weak deserializer, and then proceed to exploit it.	9.8	More Details
CVE-2021-30179	Apache Dubbo prior to 2.6.9 and 2.7.9 by default supports generic calls to arbitrary methods exposed by provider interfaces. These invocations are handled by the GenericFilter which will find the service and method specified in the first arguments of the invocation and use the Java Reflection API to make the final call. The signature for the $invoke or $invokeAsync methods is Ljava/lang/String;[Ljava/lang/String;[Ljava/lang/Object; where the first argument is the name of the method to invoke, the second one is an array with the parameter types for the method being invoked and the third one is an array with the actual call arguments. In addition, the caller also needs to set an RPC attachment specifying that the call is a generic call and how to decode the arguments. The possible values are: - true - raw.return - nativejava - bean - protobuf-json An attacker can control this RPC attachment and set it to nativejava to force the java deserialization of the byte array located in the third argument.	9.8	More Details
CVE-2021-30180	Apache Dubbo prior to 2.7.9 support Tag routing which will enable a customer to route the request to the right server. These rules are used by the customers when making a request in order to find the right endpoint. When parsing these YAML rules, Dubbo customers may enable calling arbitrary constructors.	9.8	More Details
CVE-2020-27847	A vulnerability exists in the SAML connector of the github.com/dexidp/dex library used to process SAML Signature Validation. This flaw allows an attacker to bypass SAML authentication. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. This flaw affects dex versions before 2.27.0.	9.8	More Details
CVE-2021-27852	Deserialization of Untrusted Data vulnerability in CheckboxWeb.dll of Checkbox Survey allows an unauthenticated remote attacker to execute arbitrary code. This issue affects: Checkbox Survey versions prior to 7.	9.8	More Details
CVE-2021-22731	Weak Password Recovery Mechanism for Forgotten Password vulnerability exists on Modicon Managed Switch MCSESM* and MCSESP* V8.21 and prior which could cause an unauthorized password change through HTTP / HTTPS when basic user information is known by a remote attacker.	9.8	More Details
CVE-2021-22738	Use of a Broken or Risky Cryptographic Algorithm vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior that could cause unauthorized access when credentials are discovered after a brute force attack.	9.8	More Details
CVE-2021-21986	The vSphere Client (HTML5) contains a vulnerability in a vSphere authentication mechanism for the Virtual SAN Health Check, Site Recovery, vSphere Lifecycle Manager, and VMware Cloud Director Availability plug-ins. A malicious actor with network access to port 443 on vCenter Server may perform actions allowed by the impacted plug-ins without authentication.	9.8	More Details
CVE-2021-25945	Prototype pollution vulnerability in 'js-extend' versions 0.0.1 through 1.0.1 allows attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2021-33470	COVID19 Testing Management System 1.0 is vulnerable to SQL Injection via the admin panel.	9.8	More Details
CVE-2019-25029	In Versa Director, the command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. In this attack, the attacker-supplied operating system commands are usually executed with the privileges of the vulnerable application. Command injection attacks are possible largely due to insufficient input validation.	9.8	More Details
CVE-2021-22737	Insufficiently Protected Credentials vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior that could cause unauthorized access of when credentials are discovered after a brute force attack.	9.8	More Details
CVE-2021-30181	Apache Dubbo prior to 2.6.9 and 2.7.9 supports Script routing which will enable a customer to route the request to the right server. These rules are used by the customers when making a request in order to find the right endpoint. When parsing these rules, Dubbo customers use ScriptEngine and run the rule provided by the script which by default may enable executing arbitrary code.	9.8	More Details
CVE-2021-33590	GattLib 0.3-rc1 has a stack-based buffer over-read in get_device_path_from_mac in dbus/gattlib.c.	9.8	More Details
CVE-2021-22891	A missing authorization vulnerability exists in Citrix ShareFile Storage Zones Controller before 5.7.3, 5.8.3, 5.9.3, 5.10.1 and 5.11.18 may allow unauthenticated remote compromise of the Storage Zones Controller.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22911	A improper input sanitization vulnerability exists in Rocket.Chat server 3.11, 3.12 & 3.13 that could lead to unauthenticated NoSQL injection, resulting potentially in RCE.	9.8	More Details
CVE-2021-31535	LookupCol.c in X.Org X through X11R7.7 and libX11 before 1.7.1 might allow remote attackers to execute arbitrary code. The libX11 XLookupColor request (intended for server-side color lookup) contains a flaw allowing a client to send color-name requests with a name longer than the maximum size allowed by the protocol (and also longer than the maximum packet size for normal-sized packets). The user-controlled data exceeding the maximum size is then interpreted by the server as additional X protocol requests and executed, e.g., to disable X server authorization completely. For example, if the victim encounters malicious terminal control sequences for color codes, then the attacker may be able to take full control of the running graphical session.	9.8	More Details
CVE-2021-20195	A flaw was found in keycloak in versions before 13.0.0. A Self Stored XSS attack vector escalating to a complete account takeover is possible due to user-supplied data fields not being properly encoded and Javascript code being used to process the data. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	9.6	More Details
CVE-2020-12403	A flaw was found in the way CHACHA20-POLY1305 was implemented in NSS in versions before 3.55. When using multi-part Chacha20, it could cause out-of-bounds reads. This issue was fixed by explicitly disabling multi-part ChaCha20 (which was not functioning correctly) and strictly enforcing tag length. The highest threat from this vulnerability is to confidentiality and system availability.	9.1	More Details
CVE-2018-10867	Files are accessible without restrictions from the /update/results page of redhat-certification 7 package, allowing an attacker to remove any file accessible by the apached user.	9.1	More Details
CVE-2021-27828	SQL injection in In4Suite ERP 3.2.74.1370 allows attackers to modify or delete data, causing persistent changes to the application's content or behavior by using malicious SQL queries.	9.1	More Details
CVE-2018-10866	It was discovered that the /configuration view of redhat-certification 7 does not perform an authorization check and it allows an unauthenticated user to remove a "system" file, that is an xml file with host related information, not belonging to him.	9.1	More Details
CVE-2021-20487	IBM Power9 Self Boot Engine(SBE) could allow a privileged user to inject malicious code and compromise the integrity of the host firmware bypassing the host firmware signature verification process.	9.1	More Details
CVE-2020-27832	A flaw was found in Red Hat Quay, where it has a persistent Cross-site Scripting (XSS) vulnerability when displaying a repository's notification. This flaw allows an attacker to trick a user into performing a malicious action to impersonate the target user. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	9.0	More Details
CVE-2020-15180	A flaw was found in the mysql-wsrep component of mariadb. Lack of input sanitization in `wsrep_sst_method` allows for command injection that can be exploited by a remote attacker to execute arbitrary commands on galera cluster nodes. This threatens the system's confidentiality, integrity, and availability. This flaw affects mariadb versions before 10.1.47, before 10.2.34, before 10.3.25, before 10.4.15 and before 10.5.6.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2021-22894	A buffer overflow vulnerability exists in Pulse Connect Secure before 9.1R11.4 allows a remote authenticated attacker to execute arbitrary code as the root user via ma crafted meeting room.
CVE-2020-22017	A heap-based Buffer Overflow vulnerability exists in FFmpeg 4.2 at ff_fill_rectangle in libavfilter/drawutils.c, which might lead to memory corruption and other potential consequences.
CVE-2021-22908	A buffer overflow vulnerability exists in Windows File Resource Profiles in 9.X allows a remote authenticated user with privileges to browse SMB shares to execute arbi the root user. As of version 9.1R3, this permission is not enabled by default.
CVE-2020-4520	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to inject malicious HTML code that when viewed by the authenticated victim would execute the code Force ID: 182395.
CVE-2021-22899	A command injection vulnerability exists in Pulse Connect Secure before 9.1R11.4 allows a remote authenticated attacker to perform remote code execution via Windo Profiles Feature
CVE-2018-16494	In VOS and overly permissive "umask" may allow for authorized users of the server to gain unauthorized access through insecure file permissions that can result in an read, write, or execution of newly created files and directories. Insecure umask setting was present throughout the Versa servers.
CVE-2018-16495	In VOS user session identifier (authentication token) is issued to the browser prior to authentication but is not changed after the user successfully logs into the applicati issue a new session ID following a successful login introduces the possibility for an attacker to set up a trap session on the device the victim is likely to login with.
CVE-2020-26641	A Cross Site Request Forgery (CSRF) vulnerability was discovered in iCMS 7.0.16 which can allow an attacker to execute arbitrary web scripts.

CVE Number	Description
CVE-2021-20240	A flaw was found in gdk-pixbuf in versions before 2.42.0. An integer wraparound leading to an out of bounds write can occur when a crafted GIF image is loaded. An at cause applications to crash or could potentially execute code on the victim system. The highest threat from this vulnerability is to data confidentiality and integrity as we availability.
CVE-2021-29092	Unrestricted upload of file with dangerous type vulnerability in file management component in Synology Photo Station before 6.8.14-3500 allows remote authenticated u execute arbitrary code via unspecified vectors.
CVE-2020-22016	A heap-based Buffer Overflow vulnerability in FFmpeg 4.2 at libavcodec/get_bits.h when writing .mov files, which might lead to memory corruption and other potential consequences.
CVE-2021-3495	An incorrect access control flaw was found in the kiali-operator in versions before 1.33.0 and before 1.24.7. This flaw allows an attacker with a basic level of access to t deploy a kiali operand) to use this vulnerability and deploy a given image to anywhere in the cluster, potentially gaining access to privileged service account tokens. The threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-17541	Libjpeg-turbo all version have a stack-based buffer overflow in the "transform" component. A remote attacker can send a malformed jpeg file to the service and cause a execution or denial of service of the target service.
CVE-2021-32620	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In versions prior to 11.10.13, 12.6.7, and 12.10.2, a user disabled on email verification for registration canouldre-activate themself by using the activation link provided for his registration. The problem has been patched in the following ver XWiki: 11.10.13, 12.6.7, 12.10.2, 13.0. It is possible to workaround the issue by resetting the `validkey` property of the disabled XWiki users. This can be done by editin profile with object editor.
CVE-2020-22036	A heap-based Buffer Overflow vulnerability exists in FFmpeg 4.2 in filter_intra at libavfilter/vf_bwdif.c, which might lead to memory corruption and other potential consec
CVE-2021-32621	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In versions prior to 12.6.7 and 12.10.3, a user without Script or Progr right is able to execute script requiring privileges by editing gadget titles in the dashboard. The issue has been patched in XWiki 12.6.7, 12.10.3 and 13.0RC1.
CVE-2020-26668	A SQL injection vulnerability was discovered in /core/feeds/custom.php in BigTree CMS 4.4.10 and earlier which allows an authenticated attacker to inject a malicious S the applications via the 'Create New Feed' function.
CVE-2020-26670	A vulnerability has been discovered in BigTree CMS 4.4.10 and earlier which allows an authenticated attacker to execute arbitrary commands through a crafted reques server via the 'Create a New Setting' function.
CVE-2020-22022	A heap-based Buffer Overflow vulnerability exists in FFmpeg 4.2 in filter_frame at libavfilter/vf_fieldorder.c, which might lead to memory corruption and other potential consequences.
CVE-2020-22023	A heap-based Buffer Overflow vulnerabililty exists in FFmpeg 4.2 in filter_frame at libavfilter/vf_bitplanenoise.c, which might lead to memory corruption and other poten consequences.
CVE-2020-22025	A heap-based Buffer Overflow vulnerability exists in gaussian_blur at libavfilter/vf_edgedetect.c, which might lead to memory corruption and other potential consequenc
CVE-2020-22027	A heap-based Buffer Overflow vulnerability exits in FFmpeg 4.2 in deflate16 at libavfilter/vf_neighbor.c, which might lead to memory corruption and other potential cons
CVE-2021-32924	Invision Community (aka IPS Community Suite) before 4.6.0 allows eval-based PHP code injection by a moderator because the IPS\cms\modules\front\pages_builder::previewBlock method interacts unsafely with the IPS_Theme::runProcessFunction method.
CVE-2020-22035	A heap-based Buffer Overflow vulnerability exists in FFmpeg 4.2 in get_block_row at libavfilter/vf_bm3d.c, which might lead to memory corruption and other potential consequences.
CVE-2020-22032	A heap-based Buffer Overflow vulnerability exists FFmpeg 4.2 at libavfilter/vf_edgedetect.c in gaussian_blur, which might lead to memory corruption and other potentia consequences.
CVE-2021-20026	A vulnerability in the SonicWall NSM On-Prem product allows an authenticated attacker to perform OS command injection using a crafted HTTP request. This vulnerab NSM On-Prem 2.2.0-R10 and earlier versions.
CVE-2020-22015	Buffer Overflow vulnerability in FFmpeg 4.2 in mov_write_video_tag due to the out of bounds in libavformat/movenc.c, which could let a remote malicious user obtain se information, cause a Denial of Service, or execute arbitrary code.

CVE Number	Description
CVE-2020-22034	A heap-based Buffer Overflow vulnerability exists FFmpeg 4.2 at libavfilter/vf_floodfill.c, which might lead to memory corruption and other potential consequences.
CVE-2021-24311	The wp_ajax_upload-remote-file AJAX action of the External Media WordPress plugin before 1.0.34 was vulnerable to arbitrary file uploads via any authenticated users
CVE-2021-32652	Nextcloud Mail is a mail app for the Nextcloud platform. A missing permission check in Nextcloud Mail before 1.4.3 and 1.8.2 allows another authenticated users to acc metadata of other users. Versions 1.4.3 and 1.8.2 contain patches for this vulnerability; no workarounds other than the patches are known to exist.
CVE-2019-14836	A vulnerability was found that the 3scale dev portal does not employ mechanisms for protection against login CSRF. An attacker could use this flaw to access unauthor information or conduct further attacks.
CVE-2020-22030	A heap-based Buffer Overflow vulnerability exists in FFmpeg 4.2 at libavfilter/af_afade.c in crossfade_samples_fltp, which might lead to memory corruption and other p consequences.
CVE-2020-1716	A flaw was found in the ceph-ansible playbook where it contained hardcoded passwords that were being used as default passwords while deploying Ceph services. An authenticated attacker can abuse this flaw to brute-force Ceph deployments, and gain administrator access to Ceph clusters via the Ceph dashboard to initiate read, wr delete Ceph clusters and also modify Ceph cluster configurations. Versions before ceph-ansible 6.0.0alpha1 are affected.
CVE-2021-33591	An exposed remote debugging port in Naver Comic Viewer prior to 1.0.15.0 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2020-26677	Any user logged in to a vFairs 3.3 virtual conference or event can perform SQL injection with a malicious query to the API.
CVE-2020-26678	vFairs 3.3 is affected by Remote Code Execution. Any user logged in to a vFairs virtual conference or event can abuse the functionality to upload a profile picture in orc malicious PHP file on the server and gain code execution.
CVE-2021-32027	A flaw was found in postgresql in versions before 13.3, before 12.7, before 11.12, before 10.17 and before 9.6.22. While modifying certain SQL array values, missing b checks let authenticated database users write arbitrary bytes to a wide area of server memory. The highest threat from this vulnerability is to data confidentiality and int as system availability.
CVE-2020-22029	A heap-based Buffer Overflow vulnerability exists in FFmpeg 4.2 at libavfilter/vf_colorconstancy.c: in slice_get_derivative, which crossfade_samples_fltp, which might l memory corruption and other potential consequences.
CVE-2020-22031	A Heap-based Buffer Overflow vulnerability exists in FFmpeg 4.2 at libavfilter/vf_w3fdif.c in filter16_complex_low, which might lead to memory corruption and other pot consequences.
CVE-2020-24020	Buffer Overflow vulnerability in FFMpeg 4.2.3 in dnn_execute_layer_pad in libavfilter/dnn/dnn_backend_native_layer_pad.c due to a call to memcpy without length che could let a remote malicious user execute arbitrary code.
CVE-2021-32656	Nextcloud Server is a Nextcloud package that handles data storage. A vulnerability in federated share exists in versions prior to 19.0.11, 20.0.10, and 21.0.2. An attack access to basic information about users of a server by accessing a public link that a legitimate server user added as a federated share. This happens because Nextclou sharing registered users with other Nextcloud servers, which can be done automatically when selecting the "Add server automatically once a federated share was creat successfully" setting. The vulnerability is patched in versions 19.0.11, 20.0.10, and 21.0.2 As a workaround, disable "Add server automatically once a federated share v successfully" in the Nextcloud settings.
CVE-2021-30465	runc before 1.0.0-rc95 allows a Container Filesystem Breakout via Directory Traversal. To exploit the vulnerability, an attacker must be able to create multiple container specific mount configuration. The problem occurs via a symlink-exchange attack that relies on a race condition.
CVE-2021-20492	IBM WebSphere Application Server 8.0, 8.5, 9.0, and Liberty Java Batch is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A re attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 197793.
CVE-2020-4300	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vuln expose sensitive information or consume memory resources. IBM X-Force ID: 176607.

CVE Number	Description
CVE-2021-29492	Envoy is a cloud-native edge/middle/service proxy. Envoy does not decode escaped slash sequences `%2F` and `%5C` in HTTP URL paths in versions 1.18.2 and bef remote attacker may craft a path with escaped slashes, e.g. `/something%2F..%2Fadmin`, to bypass access control, e.g. a block on `/admin`. A backend server could t slash sequences and normalize path and provide an attacker access beyond the scope provided for by the access control policy. ### Impact Escalation of Privileges w RBAC or JWT filters with enforcement based on URL path. Users with back end servers that interpret `%2F` and `/` and `%5C` and `\` interchangeably are impacted. #: Vector URL paths containing escaped slash characters delivered by untrusted client. Patches in versions 1.18.3, 1.17.3, 1.16.4, 1.15.5 contain new path normalization decode escaped slash characters. As a workaround, if back end servers treat `%2F` and `/` and `%5C` and `\` interchangeably and a URL path based access control is one may reconfigure the back end server to not treat `%2F` and `/` and `%5C` and `\` interchangeably.
CVE-2021-32616	1CDN is open-source file sharing software. In 1CDN before commit f88a2730fa50fc2c2aeab09011f6f142fd90ec25, there is a basic cross-site scripting vulnerability that attacker to inject /<script>//code</script> and execute JavaScript code on the client side.
CVE-2021-32654	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.11, 20.0.10, and 21.0.2, an attacker is able to receive write/read privileges Federated File Share. Since public links can be added as federated file share, this can also be exploited on any public link. Users can upgrade to patched versions (19. or 21.0.2) or, as a workaround, disable federated file sharing.
CVE-2021-32647	Emissary is a P2P based data-driven workflow engine. Affected versions of Emissary are vulnerable to post-authentication Remote Code Execution (RCE). The [`Creat (https://github.com/NationalSecurityAgency/emissary/blob/30c54ef16c6eb6ed09604a929939fb9f66868382/src/main/java/emissary/server/mvc/internal/CreatePlaceActi REST endpoint accepts an `sppClassName` parameter which is used to load an arbitrary class. This class is later instantiated using a constructor with the following sig `<constructor>(String, String, String)`. An attacker may find a gadget (class) in the application classpath that could be used to achieve Remote Code Execution (RCE) application. Even though the chances to find a gadget (class) that allow arbitrary code execution are low, an attacker can still find gadgets that could potentially crash th or leak sensitive data. As a work around disable network access to Emissary from untrusted sources.
CVE-2021-33183	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability container volume management component in Synology Docker before 18.09.0- local users to read or write arbitrary files via unspecified vectors.
CVE-2021-22118	In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the ter storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with mu request data.
CVE-2021-27488	Datakit Software libraries CatiaV5_3dRead, CatiaV6_3dRead, Step3dRead, Ug3dReadPsr, Jt3dReadPsr modules in KeyShot Versions v10.1 and prior lack proper vali user-supplied data when parsing CATPart files. This could result in an out-of-bounds write past the end of an allocated structure. An attacker could leverage this vulner execute code in the context of the current process.
CVE-2021-27494	Datakit Software libraries CatiaV5_3dRead, CatiaV6_3dRead, Step3dRead, Ug3dReadPsr, Jt3dReadPsr modules in KeyShot Versions v10.1 and prior lack proper vali user-supplied data when parsing STP files. This could result in a stack-based buffer overflow. An attacker could leverage this vulnerability to execute code in the contex current process.
CVE-2020-10695	An insecure modification flaw in the /etc/passwd file was found in the redhat-sso-7 container. An attacker with access to the container can use this flaw to modify the /et and escalate their privileges.
CVE-2009-3721	Multiple directory traversal and buffer overflow vulnerabilities were discovered in yTNEF, and in Evolution's TNEF parser that is derived from yTNEF. A crafted email co these applications to write data in arbitrary locations on the filesystem, crash, or potentially execute arbitrary code when decoding attachments.
CVE-2010-3843	The GTK version of ettercap uses a global settings file at /tmp/.ettercap_gtk and does not verify ownership of this file. When parsing this file for settings in gtkui_conf_re (src/interfacesgtk/ec_gtk_conf.c), an unchecked sscanf() call allows a maliciously placed settings file to overflow a statically-sized buffer on the stack.
CVE-2021-27032	Autodesk Licensing Installer was found to be vulnerable to privilege escalation issues. A malicious user with limited privileges could run any number of tools on a syste services that are configured with weak permissions and are running under elevated privileges. These weak permissions could allow all users on the operating system to service configuration and take ownership of the service.
CVE-2013-4536	An user able to alter the savevm data (either on the disk or over the wire during migration) could use this flaw to to corrupt QEMU process memory on the (destination) could potentially result in arbitrary code execution on the host with the privileges of the QEMU process.
CVE-2021-33200	kernel/bpf/verifier.c in the Linux kernel through 5.12.7 enforces incorrect limits for pointer arithmetic operations, aka CID-bb01a1bba579. This can be abused to perform bounds reads and writes in kernel memory, leading to local privilege escalation to root. In particular, there is a corner case where the off reg causes a masking direction which then results in an incorrect final aux->alu_limit.
CVE-2021-30472	A flaw was found in PoDoFo 0.9.7. A stack-based buffer overflow in PdfEncryptMD5Base::ComputeOwnerKey function in PdfEncrypt.cpp is possible because of a impr of the keyLength value.
CVE-2021-30498	A flaw was found in libcaca. A heap buffer overflow in export.c in function export_tga might lead to memory corruption and other potential consequences.
CVE-2021-30499	A flaw was found in libcaca. A buffer overflow of export.c in function export_troff might lead to memory corruption and other potential consequences.

CVE Number	Description
CVE-2021-30500	Null pointer dereference was found in upx PackLinuxElf::canUnpack() in p_lx_elf.cpp,in version UPX 4.0.0. That allow attackers to execute arbitrary code and cause a d service via a crafted file.
CVE-2021-31155	Failure to normalize the umask in please before 0.4 allows a local attacker to gain full root privileges if they are allowed to execute at least one command.
CVE-2021-31154	pleaseedit in please before 0.4 uses predictable temporary filenames in /tmp and the target directory. This allows a local attacker to gain full root privileges by staging a attack.
CVE-2021-32458	Trend Micro Home Network Security version 6.6.604 and earlier is vulnerable to an iotcl stack-based buffer overflow vulnerability which could allow an attacker to issue crafted iotcl which could lead to code execution on affected devices. An attacker must first obtain the ability to execute low-privileged code on the target device in order this vulnerability.
CVE-2021-27490	Datakit Software libraries CatiaV5_3dRead, CatiaV6_3dRead, Step3dRead, Ug3dReadPsr, Jt3dReadPsr modules in KeyShot Versions v10.1 and prior are vulnerable t bounds read, which may allow an attacker to execute arbitrary code.
CVE-2021-22907	An improper access control vulnerability exists in Citrix Workspace App for Windows potentially allows privilege escalation in CR versions prior to 2105 and 1912 LTSR CU4.
CVE-2021-29665	IBM Security Verify Access 20.07 is vulnerable to a stack based buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arb on the system with elevated privileges.
CVE-2021-27496	Datakit Software libraries CatiaV5_3dRead, CatiaV6_3dRead, Step3dRead, Ug3dReadPsr, Jt3dReadPsr modules in KeyShot Versions v10.1 and prior lack proper vali user-supplied data when parsing PRT files. This could lead to pointer dereferences of a value obtained from an untrusted source. An attacker could leverage this vulne execute code in the context of the current process.
CVE-2018-16497	In Versa Analytics, the cron jobs are used for scheduling tasks by executing commands at specific dates and times on the server. If the job is run as the user root, there potential privilege escalation vulnerability. In this case, the job runs a script as root that is writable by users who are members of the versa group.
CVE-2019-4588	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to execute arbitrary code and conduct DL attacks.
CVE-2021-29088	Improper limitation of a pathname to a restricted directory ('Path Traversal') in cgi component in Synology DiskStation Manager (DSM) before 6.2.4-25553 allows local u execute arbitrary code via unspecified vectors.
CVE-2021-22732	Improper Privilege Management vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could cause a code execution issue when an loads unauthorized code on the web server.
CVE-2021-22705	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause denial of service or unauthorized access to system inform interacting directly with a driver installed by Vijeo Designer or EcoStruxure Machine Expert
CVE-2021-22543	An issue was discovered in Linux: KVM through Improper handling of VM_IOlVM_PFNMAP vmas in KVM can bypass RO checks and can lead to pages being freed wh accessible by the VMM and guest. This allows users with the ability to start and control a VM to read/write random pages of memory and can result in local privilege es
CVE-2021-3516	There's a flaw in libxml2's xmllint in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by xmllint could trigger a use-after-free. The impact of this flaw is to confidentiality, integrity, and availability.
CVE-2020-15076	Private Tunnel installer for macOS version 3.0.1 and older versions may corrupt system critical files it should not have access via symlinks in /tmp.
CVE-2020-10145	The Adobe ColdFusion installer fails to set a secure access-control list (ACL) on the default installation directory, such as C:\ColdFusion2021\. By default, unprivileged create files in this directory structure, which creates a privilege-escalation vulnerability.
CVE-2020-25669	A vulnerability was found in the Linux Kernel where the function sunkbd_reinit having been scheduled by sunkbd_interrupt before sunkbd being freed. Though the dang is set to NULL in sunkbd_disconnect, there is still an alias in sunkbd_reinit causing Use After Free.
CVE-2020-27815	A flaw was found in the JFS filesystem code in the Linux Kernel which allows a local attacker with the ability to set extended attributes to panic the system, causing mer corruption or escalating privileges. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.

CVE Number	Description
CVE-2020-25671	A vulnerability was found in Linux Kernel, where a refcount leak in llcp_sock_connect() causing use-after-free which might lead to privilege escalations.
CVE-2021-32457	Trend Micro Home Network Security version 6.6.604 and earlier is vulnerable to an iotcl stack-based buffer overflow vulnerability which could allow an attacker to issue crafted iotcl to escalate privileges on affected devices. An attacker must first obtain the ability to execute low-privileged code on the target device in order to exploit this
CVE-2021-23019	The NGINX Controller 2.0.0 thru 2.9.0 and 3.x before 3.15.0 Administrator password may be exposed in the systemd.txt file that is included in the NGINX support packa
CVE-2020-25670	A vulnerability was found in Linux Kernel where refcount leak in llcp_sock_bind() causing use-after-free which might lead to privilege escalations.
CVE-2021-29740	IBM Spectrum Scale 5.0.0 through 5.0.5.6 and 5.1.0 through 5.1.0.3 system core component is affected by a format string security vulnerability. An attacker could exec code in the context of process memory, potentially escalating their system privileges and taking control over the entire system with root access. IBM X-Force ID: 20147
CVE-2021-22733	Improper Privilege Management vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could cause shell access when unauthorized loaded into the system folder.
CVE-2021-23017	A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrit in worker process crash or potential other impact.
CVE-2021-33184	Server-Side request forgery (SSRF) vulnerability in task management component in Synology Download Station before 3.8.15-3563 allows remote authenticated users arbitrary files via unspecified vectors.
CVE-2021-22123	An OS command injection vulnerability in FortiWeb's management interface 6.3.7 and below, 6.2.3 and below, 6.1.x, 6.0.x, 5.9.x may allow a remote authenticated atta execute arbitrary commands on the system via the SAML server configuration page.
CVE-2021-33558	Boa 0.94.13 allows remote attackers to obtain sensitive information via a misconfiguration involving backup.html, preview.html, js/log.js, log.html, email.html, online-use config.js. NOTE: multiple third parties report that this is a site-specific issue because those files are not part of Boa.
CVE-2021-29629	In FreeBSD 13.0-STABLE before n245765-bec0d2c9c841, 12.2-STABLE before r369859, 11.4-STABLE before r369866, 13.0-RELEASE before p1, 12.2-RELEASE be 11.4-RELEASE before p10, missing message validation in libradius(3) could allow malicious clients or servers to trigger denial of service in vulnerable servers or clients respectively.
CVE-2018-10865	It was discovered that the /configuration view of redhat-certification 7 does not perform an authorization check and it allows an unauthenticated user to call a "restart" R on any host accessible by the system, even if not belonging to him.
CVE-2018-10868	redhat-certification 7 does not properly restrict the number of recursive definitions of entities in XML documents, allowing an unauthenticated user to run a "Billion Laugh replying to XMLRPC methods when getting the status of an host.
CVE-2021-22909	A vulnerability found in EdgeMAX EdgeRouter V2.0.9 and earlier could allow a malicious actor to execute a man-in-the-middle (MitM) attack during a firmware update. vulnerability is fixed in EdgeMAX EdgeRouter V2.0.9-hotfix.1 and later.
CVE-2021-22892	An information disclosure vulnerability exists in the Rocket.Chat server fixed v3.13, v3.12.2 & v3.11.3 that allowed email addresses to be disclosed by enumeration and checks.
CVE-2021-28651	An issue was discovered in Squid before 4.15 and 5.x before 5.0.6. Due to a buffer-management bug, it allows a denial of service. When resolving a request with the u the parser leaks a small amount of memory. However, there is an unspecified attack methodology that can easily trigger a large amount of memory consumption.
CVE-2021-22885	A possible information disclosure / unintended method execution vulnerability in Action Pack >= 2.0.0 when using the `redirect_to` or `polymorphic_url`helper with untru input.
CVE-2021-33194	golang.org/x/net before v0.0.0-20210520170846-37e1c6afe023 allows attackers to cause a denial of service (infinite loop) via crafted ParseFragment input.
CVE-2021-31702	Frontier ichris through 5.18 mishandles making a DNS request for the hostname in the HTTP Host header, as demonstrated by submitting 127.0.0.1 multiple times for D

CVE Number	Description
CVE-2021-33623	The trim-newlines package before 3.0.1 and 4.x before 4.0.1 for Node.js has an issue related to regular expression denial-of-service (ReDoS) for the .end() method.
CVE-2018-10863	It was discovered that redhat-certification 7 is not properly configured and it lists all files and directories in the /var/www/rhcert/store/transfer directory, through the /rhce URL. An unauthorized attacker may use this flaw to gather sensible information.
CVE-2021-22699	Improper Input Validation vulnerability exists in Modicon M241/M251 logic controllers firmware prior to V5.1.9.1 that could cause denial of service when specific crafted sent to the controller over HTTP.
CVE-2021-33038	An issue was discovered in management/commands/hyperkitty_import.py in HyperKitty through 1.3.4. When importing a private mailing list's archives, these archives a visible for the duration of the import. For example, sensitive information might be available on the web for an hour during a large migration from Mailman 2 to Mailman 3
CVE-2020-1920	A regular expression denial of service (ReDoS) vulnerability in the validateBaseUrl function can cause the application to use excessive resources, become unresponsiv This was introduced in react-native version 0.59.0 and fixed in version 0.64.1.
CVE-2021-33587	The css-what package 4.0.0 through 5.0.0 for Node.js does not ensure that attribute parsing has Linear Time Complexity relative to the size of the input.
CVE-2021-22359	There is a denial of service vulnerability in the verisions V200R005C00SPC500 of S5700 and V200R005C00SPC500 of S6700. An attacker could exploit this vulnerabi sending specific message to a targeted device. Due to insufficient input validation, successful exploit can cause the service abnormal.
CVE-2021-20576	IBM Security Verify Access 20.07 could allow a remote attacker to send a specially crafted HTTP GET request that could cause the application to crash.
CVE-2020-18395	A NULL-pointer deference issue was discovered in GNU_gama::set() in ellipsoid.h in Gama 2.04 which can lead to a denial of service (DOS) via segment faults caused inputs.
CVE-2021-29628	In FreeBSD 13.0-STABLE before n245764-876ffe28796c, 12.2-STABLE before r369857, 13.0-RELEASE before p1, and 12.2-RELEASE before p7, a system call trigge could cause SMAP protections to be disabled for the duration of the system call. This weakness could be combined with other kernel bugs to craft an exploit.
CVE-2021-29505	XStream is software for serializing Java objects to XML and back again. A vulnerability in XStream versions prior to 1.4.17 may allow a remote attacker has sufficient ri execute commands of the host only by manipulating the processed input stream. No user who followed the recommendation to setup XStream's security framework wit limited to the minimal required types is affected. The vulnerability is patched in version 1.4.17.
CVE-2021-22736	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which a denial of service when an unauthorized file is uploaded.
CVE-2019-4724	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain credentials from a user's browser via incorrect autocomplete settings in New Content Back IBM X-Force ID: 172130.
CVE-2020-25710	A flaw was found in OpenLDAP in versions before 2.4.56. This flaw allows an attacker who sends a malicious packet processed by OpenLDAP to force a failed assertio csnNormalize23(). The highest threat from this vulnerability is to system availability.
CVE-2019-4723	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain credentials from a user's browser via incorrect autocomplete settings in New Data Server C page. IBM X-Force ID: 172129.
CVE-2021-31684	A vulnerability was discovered in the indexOf function of JSONParserByteArray in JSON Smart versions 1.3 and 2.4 which causes a denial of service (DOS) via a craft request.
CVE-2021-20237	An uncontrolled resource consumption (memory leak) flaw was found in ZeroMQ's src/xpub.cpp in versions before 4.3.3. This flaw allows a remote unauthenticated atta crafted PUB messages that consume excessive memory if the CURVE/ZAP authentication is disabled on the server, causing a denial of service. The highest threat fro vulnerability is to system availability.
CVE-2021-33506	jitsi-meet-prosody in Jitsi Meet before 2.0.5963-1 does not ensure that restrict_room_creation is set by default. This can allow an attacker to circumvent conference mo
CVE-2021-23018	Intra-cluster communication does not use TLS. The services within the NGINX Controller 3.x before 3.4.0 namespace are using cleartext protocols inside the cluster.

CVE Number	Description
CVE-2020-17514	Apache Fineract prior to 1.5.0 disables HTTPS hostname verification in ProcessorHelper in the configureClient method. Under typical deployments, a man in the middle could be successful.
CVE-2020-14387	A flaw was found in rsync in versions since 3.2.0pre1. Rsync improperly validates certificate with host mismatch vulnerability. A remote, unauthenticated attacker could flaw by performing a man-in-the-middle attack using a valid certificate for another hostname which could compromise confidentiality and integrity of data transmitted usi The highest threat from this vulnerability is to data confidentiality and integrity. This flaw affects rsync versions before 3.2.4.
CVE-2021-25217	In ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16, ISC DHCP 4.4.0 -> 4.4.2 (Other branches of ISC DHCP (i.e., releases in the 4.0.x series or lower and releases in the 4.3.x beyond their End-of-Life (EOL) and no longer supported by ISC. From inspection it is clear that the defect is also present in releases from those series, but they have n officially tested for the vulnerability), The outcome of encountering the defect while reading a lease that will trigger it varies, according to: the component being affected or dhcpd) whether the package was built as a 32-bit or 64-bit binary whether the compiler flag -fstack-protection-strong was used when compiling In dhclient, ISC has n successfully reproduced the error on a 64-bit system. However, on a 32-bit system it is possible to cause dhclient to crash when reading an improper lease, which coul network connectivity problems for an affected system due to the absence of a running DHCP client process. In dhcpd, when run in DHCPv4 or DHCPv6 mode: if the dh binary was built for a 32-bit architecture AND the -fstack-protection-strong flag was specified to the compiler, dhcpd may exit while parsing a lease file containing an obj lease, resulting in lack of service to clients. Additionally, the offending lease and the lease immediately following it in the lease database may be improperly deleted. if t server binary was built for a 64-bit architecture OR if the -fstack-protection-strong compiler flag was NOT specified, the crash will not occur, but it is possible for the offe and the lease which immediately followed it to be improperly deleted.
CVE-2021-3412	It was found that all versions of 3Scale developer portal lacked brute force protections. An attacker could use this gap to bypass login controls, and access privileged in possibly conduct further attacks.
CVE-2021-33180	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in cgi component in Synology Media Server before 1.8.1-2876 allow attackers to execute arbitrary SQL commands via unspecified vectors.
CVE-2021-24312	The parameters $cache_path, $wp_cache_debug_ip, $wp_super_cache_front_page_text, $cache_scheduled_time, $cached_direct_pages used in the settings of WP WordPress plugin before 1.7.3 result in RCE because they allow input of '$' and '\n'. This is due to an incomplete fix of CVE-2021-24209.
CVE-2021-22735	Improper Verification of Cryptographic Signature vulnerability exists inhomeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could allow remote code exec unauthorized code is copied to the device.
CVE-2021-22734	Improper Verification of Cryptographic Signature vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could cause remote code exe an attacker loads unauthorized code.
CVE-2021-22900	A vulnerability allowed multiple unrestricted uploads in Pulse Connect Secure before 9.1R11.4 that could lead to an authenticated administrator to perform a file write vi maliciously crafted archive upload in the administrator web interface.
CVE-2021-32614	A flaw was found in dmg2img through 20170502. fill_mishblk() does not check the length of the read buffer, and copy 0xCC bytes from it. The length of the buffer is cor attacker. By providing a length smaller than 0xCC, memcpy reaches out of the malloc'ed bound. This possibly leads to memory layout information leaking in the data. T used in a chain of vulnerability in order to reach code execution.
CVE-2021-20267	A flaw was found in openstack-neutron's default Open vSwitch firewall rules. By sending carefully crafted packets, anyone in control of a server instance connected to t switch can impersonate the IPv6 addresses of other systems on the network, resulting in denial of service or in some cases possibly interception of traffic intended for d destinations. Only deployments using the Open vSwitch driver are affected. Source: OpenStack project. Versions before openstack-neutron 15.3.3, openstack-neutron openstack-neutron 17.1.1 are affected.
CVE-2021-3561	An Out of Bounds flaw was found fig2dev version 3.2.8a. A flawed bounds check in read_objects() could allow an attacker to provide a crafted malicious input causing t application to either crash or in some cases cause memory corruption. The highest threat from this vulnerability is to integrity as well as system availability.
CVE-2019-4730	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vuln expose sensitive information or consume memory resources. IBM X-Force ID: 172533.
CVE-2020-10709	A security flaw was found in Ansible Tower when requesting an OAuth2 token with an OAuth2 application. Ansible Tower uses the token to provide authentication. This an attacker to obtain a refresh token that does not expire. The original token granted to the user still has access to Ansible Tower, which allows any user that can gain a token to be fully authenticated to Ansible Tower. This flaw affects Ansible Tower versions before 3.6.4 and Ansible Tower versions before 3.5.6.
CVE-2021-3549	An out of bounds flaw was found in GNU binutils objdump utility version 2.36. An attacker could use this flaw and pass a large section to avr_elf32_load_records_from_ probably resulting in a crash or in some cases memory corruption. The highest threat from this vulnerability is to integrity as well as system availability.
CVE-2021-3548	A flaw was found in dmg2img through 20170502. dmg2img did not validate the size of the read buffer during memcpy() inside the main() function. This possibly leads to layout information leaking in the data. This might be used in a chain of vulnerability in order to reach code execution.
CVE-2020-25668	A flaw was found in Linux Kernel because access to the global variable fg_console is not properly synchronized leading to a use after free in con_font_op.

CVE Number	Description
CVE-2020-25697	A privilege escalation flaw was found in the Xorg-x11-server due to a lack of authentication for X11 clients. This flaw allows an attacker to take control of an X applicatio impersonating the server it is expecting to connect to.
CVE-2021-32642	radsecproxy is a generic RADIUS proxy that supports both UDP and TLS (RadSec) RADIUS transports. Missing input validation in radsecproxy's `naptr-eduroam.sh` a dynsrv.sh` scripts can lead to configuration injection via crafted radsec peer discovery DNS records. Users are subject to Information disclosure, Denial of Service, Red Radius connection to a non-authenticated server leading to non-authenticated network access. Updated example scripts are available in the master branch and 1.9 rele that the scripts are not part of the installation package and are not updated automatically. If you are using the examples, you have to update them manually. The dyndis work independently of the radsecproxy code. The updated scripts can be used with any version of radsecproxy.
CVE-2021-31924	Yubico pam-u2f before 1.1.1 has a logic issue that, depending on the pam-u2f configuration and the application used, could lead to a local PIN bypass. This issue does user presence (touch) or cryptographic signature verification to be bypassed, so an attacker would still need to physically possess and interact with the YubiKey or anot authenticator. If pam-u2f is configured to require PIN authentication, and the application using pam-u2f allows the user to submit NULL as the PIN, pam-u2f will attempt FIDO2 authentication without PIN. If this authentication is successful, the PIN requirement is bypassed.
CVE-2020-35506	A use-after-free vulnerability was found in the am53c974 SCSI host bus adapter emulation of QEMU in versions before 6.0.0 during the handling of the 'Information Tra command (CMD_TI). This flaw allows a privileged guest user to crash the QEMU process on the host, resulting in a denial of service or potential code execution with th of the QEMU process.
CVE-2021-22741	Use of Password Hash with Insufficient Computational Effort vulnerability exists in ClearSCADA (all versions), EcoStruxure Geo SCADA Expert 2019 (all versions), and EcoStruxure Geo SCADA Expert 2020 (V83.7742.1 and prior), which could cause the revealing of account credentials when server database files are available. Exposu files to an attacker can make the system vulnerable to password decryption attacks. Note that ".sde" configuration export files do not contain user account password ha
CVE-2021-20292	There is a flaw reported in the Linux kernel in versions before 5.9 in drivers/gpu/drm/nouveau/nouveau_sgdma.c in nouveau_sgdma_create_ttm in Nouveau DRM subs issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker with a local account with a root privilege, can this vulnerability to escalate privileges and execute code in the context of the kernel.
CVE-2021-3515	A shell injection flaw was found in pglogical in versions before 2.3.4 and before 3.6.26. An attacker with CREATEDB privileges on a PostgreSQL server can craft a data that allows execution of shell commands as the postgresql user when calling pglogical.create_subscription().
CVE-2021-3543	A flaw null pointer dereference in the Nitro Enclaves kernel driver was found in the way that Enclaves VMs forces closures on the enclave file descriptor. A local user of machine could use this flaw to crash the system or escalate their privileges on the system.
CVE-2021-33181	Server-Side Request Forgery (SSRF) vulnerability in webapi component in Synology Video Station before 2.4.10-1632 allows remote authenticated users to send arbitr to intranet resources via unspecified vectors.
CVE-2020-22026	Buffer Overflow vulnerability exists in FFmpeg 4.2 in the config_input function at libavfilter/af_tremolo.c, which could let a remote malicious user cause a Denial of Servi
CVE-2021-31808	An issue was discovered in Squid before 4.15 and 5.x before 5.0.6. Due to an input-validation bug, it is vulnerable to a Denial of Service attack (against all clients using A client sends an HTTP Range request to trigger this.
CVE-2020-1701	A flaw was found in the KubeVirt main virt-handler versions before 0.26.0 regarding the access permissions of virt-handler. An attacker with access to create VMs could secret within their namespace, allowing them to read the contents of that secret.
CVE-2021-24333	The Content Copy Protection & Prevent Image Save WordPress plugin through 1.3 does not check for CSRF when saving its settings, not perform any validation and s them, allowing attackers to make a logged in administrator set arbitrary XSS payloads in them.
CVE-2021-26111	A missing release of memory after effective lifetime vulnerability in FortiSwitch 6.4.0 to 6.4.6, 6.2.0 to 6.2.6, 6.0.0 to 6.0.6, 3.6.11 and below may allow an attacker on a network to exhaust available memory by sending specifically crafted LLDP/CDP/EDP packets to the device.
CVE-2021-31642	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a rel device.
CVE-2020-22044	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the url_open_dyn_buf_internal function in libavformat/aviobuf.c.
CVE-2021-32543	The CTS Web transaction system related to authentication management is implemented incorrectly. After login, remote attackers can manipulate cookies to access oth and trade in the stock market with spoofed identity.
CVE-2021-33408	Local File Inclusion vulnerability in Ab Initio Control>Center before 4.0.2.6 allows remote attackers to retrieve arbitrary files. Fixed in v4.0.2.6 and v4.0.3.1.
CVE-2021-33620	Squid before 4.15 and 5.x before 5.0.6 allows remote servers to cause a denial of service (affecting availability to all clients) via an HTTP response. The issue trigger is that can be expected to exist in HTTP traffic without any malicious intent by the server.

CVE Number	Description
CVE-2021-22740	Information Exposure vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could cause information to be exposed when an unautho uploaded.
CVE-2020-22028	Buffer Overflow vulnerability exists in FFmpeg 4.2 in filter_vertically_8 at libavfilter/vf_avgblur.c, which could cause a remote Denial of Service.
CVE-2020-22020	Buffer Overflow vulnerability in FFmpeg 4.2 in the build_diff_map function in libavfilter/vf_fieldmatch.c, which could let a remote malicious user cause a Denial of Servic
CVE-2020-22019	Buffer Overflow vulnerability in FFmpeg 4.2 at convolution_y_10bit in libavfilter/vf_vmafmotion.c, which could let a remote malicious user cause a Denial of Service.
CVE-2020-27748	A flaw was found in the xdg-email component of xdg-utils-1.1.0-rc1 and newer. When handling mailto: URIs, xdg-email allows attachments to be discreetly added via th being passed to Thunderbird. An attacker could potentially send a victim a URI that automatically attaches a sensitive file to a new email. If a victim user does not notic attachment was added and sends the email, this could result in sensitive information disclosure. It has been confirmed that the code behind this issue is in xdg-email ar Thunderbird.
CVE-2021-20486	IBM Cloud Pak for Data 3.0 could allow an authenticated user to obtain sensitive information when installed with additional plugins. IBM X-Force ID: 197668.
CVE-2021-26034	An issue was discovered in Joomla! 3.0.0 through 3.9.26. A missing token check causes a CSRF vulnerability in data download endpoints in com_banners and com_sy
CVE-2021-26033	An issue was discovered in Joomla! 3.0.0 through 3.9.26. A missing token check causes a CSRF vulnerability in the AJAX reordering endpoint.
CVE-2021-24318	The Listeo WordPress theme before 1.6.11 did not ensure that the Post/Page and Booking to delete belong to the user making the request, allowing any authenticated delete arbitrary page/post and booking via an IDOR vector.
CVE-2020-22021	Buffer Overflow vulnerability in FFmpeg 4.2 at filter_edges function in libavfilter/vf_yadif.c, which could let a remote malicious user cause a Denial of Service.
CVE-2020-22024	Buffer Overflow vulnerability in FFmpeg 4.2 at the lagfun_frame16 function in libavfilter/vf_lagfun.c, which could let a remote malicious user cause Denial of Service.
CVE-2020-14301	An information disclosure vulnerability was found in libvirt in versions before 6.3.0. HTTP cookies used to access network-based disks were saved in the XML dump of domain. This flaw allows an attacker to access potentially sensitive information in the domain configuration via the `dumpxml` command.
CVE-2020-22038	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the ff_v4l2_m2m_create_context function in v4l2_m2m.c.
CVE-2021-31806	An issue was discovered in Squid before 4.15 and 5.x before 5.0.6. Due to a memory-management bug, it is vulnerable to a Denial of Service attack (against all clients proxy) via HTTP Range request processing.
CVE-2021-22411	There is an out-of-bounds write vulnerability in some Huawei products. The code of a module have a bad judgment logic. Attackers can exploit this vulnerability by perf multiple abnormal activities to trigger the bad logic and cause out-of-bounds write. This may compromise the normal service of the module.Affected product versions in Module versions V500R005C00SPC100,V500R005C00SPC200;Secospace USG6300 versions V500R001C30SPC200,V500R001C30SPC600,V500R001C60SPC500,V500R005C00SPC100,V500R005C00SPC200;Secospace USG6500 versions V500R001C30SPC200,V500R001C30SPC600,V500R001C60SPC500,V500R005C00SPC100,V500R005C00SPC200;Secospace USG6600 versions V500R001C30SPC200,V500R001C30SPC600,V500R001C60SPC500,V500R005C00SPC100,V500R005C00SPC200;USG9500 versions V500R001C60SPC500,V500R005C00SPC100,V500R005C00SPC200.
CVE-2021-21734	Some PON MDU devices of ZTE stored sensitive information in plaintext, and users with login authority can obtain it by inputing command. This affects: ZTE PON MDU ZXA10 F821 V1.7.0P3T22, ZXA10 F822 V1.4.3T6, ZXA10 F819 V1.2.1T5, ZXA10 F832 V1.1.1T7, ZXA10 F839 V1.1.0T8, ZXA10 F809 V3.2.1T1, ZXA10 F822P V1.1. F832 V2.00.00.01
CVE-2021-3514	When using a sync_repl client in 389-ds-base, an authenticated attacker can cause a NULL pointer dereference using a specially crafted query, causing a crash.

CVE Number	Description
CVE-2021-28662	An issue was discovered in Squid 4.x before 4.15 and 5.x before 5.0.6. If a remote server sends a certain response header over HTTP or HTTPS, there is a denial of se header can plausibly occur in benign network traffic.
CVE-2020-10701	A missing authorization flaw was found in the libvirt API responsible for changing the QEMU agent response timeout. This flaw allows read-only connections to adjust th libvirt waits for the QEMU guest agent to respond to agent commands. Depending on the timeout value that is set, this flaw can make guest agent commands fail becau cannot respond in time. Unprivileged users with a read-only connection could abuse this flaw to set the response timeout for all guest agent messages to zero, potentia a denial of service. This flaw affects libvirt versions before 6.2.0.
CVE-2021-32459	Trend Micro Home Network Security version 6.6.604 and earlier contains a hard-coded password vulnerability in the log collection server which could allow an attacker specially crafted network request to lead to arbitrary authentication. An attacker must first obtain the ability to execute high-privileged code on the target device in order this vulnerability.
CVE-2020-10716	A flaw was found in Red Hat Satellite's Job Invocation, where the "User Input" entry was not properly restricted to the view. This flaw allows a malicious Satellite user to through the Job Invocation, with the ability to search for passwords and other sensitive data. This flaw affects tfm-rubygem-foreman_ansible versions before 4.0.3.4.
CVE-2021-20278	An authentication bypass vulnerability was found in Kiali in versions before 1.31.0 when the authentication strategy `OpenID` is used. When RBAC is enabled, Kiali ass some of the token validation is handled by the underlying cluster. When OpenID `implicit flow` is used with RBAC turned off, this token validation doesn't occur, and this malicious user to bypass the authentication.
CVE-2020-22037	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in avcodec_alloc_context3 at options.c.
CVE-2019-4471	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain sensitive information, caused by the failure to set the secure flag for a sensitive cookie in a session. A remote attacker could exploit this vulnerability to obtain sensitive information. IBM X-Force ID: 163780.
CVE-2021-31920	Istio before 1.8.6 and 1.9.x before 1.9.5 has a remotely exploitable vulnerability where an HTTP request path with multiple slashes or escaped slash characters (%2F o potentially bypass an Istio authorization policy when path based authorization rules are used.
CVE-2021-20196	A NULL pointer dereference flaw was found in the floppy disk emulator of QEMU. This issue occurs while processing read/write ioport commands if the selected floppy initialized with a block device. This flaw allows a privileged guest user to crash the QEMU process on the host, resulting in a denial of service. The highest threat from th vulnerability is to system availability.
CVE-2020-22039	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the inavi_add_ientry function.
CVE-2020-22040	A Denial of Service vulnerability exists in FFmpeg 4.2 idue to a memory leak in the v_frame_alloc function in frame.c.
CVE-2020-22041	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the av_buffersrc_add_frame_flags function in buffersrc.
CVE-2020-22033	A heap-based Buffer Overflow Vulnerability exists FFmpeg 4.2 at libavfilter/vf_vmafmotion.c in convolution_y_8bit, which could let a remote malicious user cause a Der Service.
CVE-2020-22042	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak is affected by: memory leak in the link_filter_inouts function in libavfilter/graphparser.c.
CVE-2020-22043	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak at the fifo_alloc_common function in libavutil/fifo.c.
CVE-2021-32635	Singularity is an open source container platform. In verions 3.7.2 and 3.7.3, Dde to incorrect use of a default URL, `singularity` action commands (`run`/`shell`/`exec`) s container using a `library://` URI will always attempt to retrieve the container from the default remote endpoint (`cloud.sylabs.io`) rather than the configured remote endp attacker may be able to push a malicious container to the default remote endpoint with a URI that is identical to the URI used by a victim with a non-default remote endp executing the malicious container. Only action commands (`run`/`shell`/`exec`) against `library://` URIs are affected. Other commands such as `pull` / `push` respect the remote endpoint. The vulnerability is patched in Singularity version 3.7.4. Two possible workarounds exist: Users can only interact with the default remote endpoint, or a installation can have an execution control list configured to restrict execution to containers signed with specific secure keys.
CVE-2021-24328	The WP Login Security and History WordPress plugin through 1.0 did not have CSRF check when saving its settings, not any sanitisation or validation on them. This co attackers to make logged in administrators change the plugin's settings to arbitrary values, and set XSS payloads on them as well
CVE-2021-25640	In Apache Dubbo prior to 2.6.9 and 2.7.9, the usage of parseURL method will lead to the bypass of white host check which can cause open redirect or SSRF vulnerabil

CVE Number	Description
CVE-2021-24335	The Car Repair Services & Auto Mechanic WordPress theme before 4.0 did not properly sanitise its serviceestimatekey search parameter before outputting it back in th leading to a reflected Cross-Site Scripting issue
CVE-2020-25715	A flaw was found in pki-core 10.9.0. A specially crafted POST request can be used to reflect a DOM-based cross-site scripting (XSS) attack to inject code into the searc which can get automatically executed. The highest threat from this vulnerability is to data integrity.
CVE-2021-24316	The search feature of the Mediumish WordPress theme through 1.0.47 does not properly sanitise it's 's' GET parameter before output it back the page, leading to the C Scripting issue.
CVE-2021-24317	The Listeo WordPress theme before 1.6.11 did not properly sanitise some parameters in its Search, Booking Confirmation and Personal Message pages, leading to Cr Scripting issues
CVE-2020-26642	A cross-site scripting (XSS) vulnerability has been discovered in the login page of SeaCMS version 11 which allows an attacker to inject arbitrary web script or HTML.
CVE-2020-10688	A cross-site scripting (XSS) flaw was found in RESTEasy in versions before 3.11.1.Final and before 4.5.3.Final, where it did not properly handle URL encoding when th RESTEASY003870 exception occurs. An attacker could use this flaw to launch a reflected XSS attack.
CVE-2021-24320	The Bello - Directory & Listing WordPress theme before 1.6.0 did not properly sanitise and escape its listing_list_view, bt_bb_listing_field_my_lat, bt_bb_listing_field_m bt_bb_listing_field_distance_value, bt_bb_listing_field_my_lat_default, bt_bb_listing_field_keyword, bt_bb_listing_field_location_autocomplete, bt_bb_listing_field_price_range_from and bt_bb_listing_field_price_range_to parameter in ints listing page, leading to reflected Cross-Site Scripting issues.
CVE-2021-31641	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpa W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated.
CVE-2021-32645	Tenancy multi-tenant is an open source multi-domain controller for the Laravel web framework. In some situations, it is possible to have open redirects where users car redirected from your site to any other site using a specially crafted URL. This is only the case for installations where the default Hostname Identification is used and the uses tenants that have `force_https` set to `true` (default: `false`). Version 5.7.2 contains the relevant patches to fix this bug. Stripping the URL from special characters specially crafted URL's from being redirected to. As a work around users can set the `force_https` to every tenant to `false`, however this may degrade connection secu
CVE-2021-3486	GLPi 9.5.4 does not sanitize the metadata. This way its possible to insert XSS into plugins to execute JavaScript code.
CVE-2021-3509	A flaw was found in Red Hat Ceph Storage 4, in the Dashboard component. In response to CVE-2020-27839, the JWT token was moved from localStorage to an httpO However, token cookies are used in the body of the HTTP response for the documentation, which again makes it available to XSS.The greatest threat to the system is t confidentiality, integrity, and availability.
CVE-2020-1761	A flaw was found in the OpenShift web console, where the access token is stored in the browser's local storage. An attacker can use this flaw to get the access token v access, or an XSS attack on the victim's browser. This flaw affects openshift/console versions before openshift/console-4.
CVE-2021-20727	Cross-site scripting vulnerability in Zettlr from 0.20.0 to 1.8.8 allows an attacker to execute an arbitrary script by loading a file or code snippet containing an invalid ifram
CVE-2021-26032	An issue was discovered in Joomla! 3.0.0 through 3.9.26. HTML was missing in the executable block list of MediaHelper::canUpload, leading to XSS attack vectors.
CVE-2020-18221	Cross Site Scripting (XSS) in Typora v0.9.65 and earlier allows remote attackers to execute arbitrary code by injecting commands during block rendering of a mathema
CVE-2020-35504	A NULL pointer dereference flaw was found in the SCSI emulation support of QEMU in versions before 6.0.0. This flaw allows a privileged guest user to crash the QEM on the host, resulting in a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2018-16499	In VOS compromised, an attacker at network endpoints can possibly view communications between an unsuspecting user and the service using man-in-the-middle atta of unapproved SSH encryption protocols or cipher suites also violates the Data Protection TSR (Technical Security Requirements).
CVE-2021-31525	net/http in Go before 1.15.12 and 1.16.x before 1.16.4 allows remote attackers to cause a denial of service (panic) via a large header to ReadRequest or ReadRespons Transport, and Client can each be affected in some configurations.
CVE-2021-22739	Information Exposure vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could cause a device to be compromised when it is first

CVE Number	Description
CVE-2021-32643	Http4s is a Scala interface for HTTP services. `StaticFile.fromUrl` can leak the presence of a directory on a server when the `URL` scheme is not `file://`, and the URL p fetchable resource under its scheme and authority. The function returns `F[None]`, indicating no resource, if `url.getFile` is a directory, without first checking the scheme of the URL. If a URL connection to the scheme and URL would return a stream, and the path in the URL exists as a directory on the server, the presence of the directo server could be inferred from the 404 response. The contents and other metadata about the directory are not exposed. This affects http4s versions: 0.21.7 through 0.21 M1 through 0.22.0-M8, 0.23.0-M1, and 1.0.0-M1 through 1.0.0-M22. The [patch](https://github.com/http4s/http4s/commit/52e1890665410b4385e37b96bc49c5e3c708e available in the following versions: v0.21.24, v0.22.0-M9, v0.23.0-M2, v1.0.0-M23. As a workaround users can avoid calling `StaticFile.fromUrl` with non-file URLs.
CVE-2021-29507	GENIVI Diagnostic Log and Trace (DLT) provides a log and trace interface. In versions of GENIVI DLT between 2.10.0 and 2.18.6, a configuration file containing the sp characters could cause a vulnerable component to crash. All the applications which are using the configuration file could fail to generate their dlt logs in system. As of ti publication, no patch exists. As a workaround, one may check the integrity of information in configuration file manually.
CVE-2021-20191	A flaw was found in ansible. Credentials, such as secrets, are being disclosed in console log by default and not protected by no_log feature when using those modules. can take advantage of this information to steal those credentials. The highest threat from this vulnerability is to data confidentiality. Versions before ansible 2.9.18 are a
CVE-2020-36372	Stack overflow vulnerability in parse_plus_minus Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.
CVE-2021-30501	An assertion abort was found in upx MemBuffer::alloc() in mem.cpp, in version UPX 4.0.0. The flow allows attackers to cause a denial of service (abort) via a crafted file
CVE-2020-18392	Stack overflow vulnerability in parse_array Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.
CVE-2021-3527	A flaw was found in the USB redirector device (usb-redir) of QEMU. Small USB packets are combined into a single, large transfer request, to reduce the overhead and performance. The combined size of the bulk transfer is used to dynamically allocate a variable length array (VLA) on the stack without proper validation. Since the total bounded, a malicious guest could use this flaw to influence the array length and cause the QEMU process to perform an excessive allocation on the stack, resulting in a service.
CVE-2020-36366	Stack overflow vulnerability in parse_value Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.
CVE-2020-36367	Stack overflow vulnerability in parse_block Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.
CVE-2020-36368	Stack overflow vulnerability in parse_statement Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.
CVE-2020-36369	Stack overflow vulnerability in parse_statement_list Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.
CVE-2018-16498	In Versa Director, the unencrypted backup files stored on the Versa deployment contain credentials stored within configuration files. These credentials are for various a components such as SNMP, and SSL and Trust keystores.
CVE-2020-36371	Stack overflow vulnerability in parse_mul_div_rem Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.
CVE-2020-36373	Stack overflow vulnerability in parse_shifts Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.
CVE-2021-20297	A flaw was found in NetworkManager in versions before 1.30.0. Setting match.path and activating a profile crashes NetworkManager. The highest threat from this vulne system availability.
CVE-2020-36374	Stack overflow vulnerability in parse_comparison Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.
CVE-2020-25673	A vulnerability was found in Linux kernel where non-blocking socket in llcp_sock_connect() leads to leak and eventually hanging-up the system.
CVE-2021-23021	The Nginx Controller 3.x before 3.7.0 agent configuration file /etc/controller-agent/agent.conf is world readable with current permission bits set to 644.

CVE Number	Description
CVE-2019-25030	In Versa Director, Versa Analytics and VOS, Passwords are not hashed using an adaptive cryptographic hash function or key derivation function prior to storage. Popul algorithms based on the Merkle-Damgardconstruction (such as MD5 and SHA-1) alone are insufficient in thwarting password cracking. Attackers can generate and use precomputed hashes for all possible password character combinations (commonly referred to as "rainbow tables") relatively quickly. The use of adaptive hashing algori asscryptorbcryptor Key-Derivation Functions (i.e.PBKDF2) to hash passwords make generation of such rainbow tables computationally infeasible.
CVE-2021-23020	The NAAS 3.x before 3.10.0 API keys were generated using an insecure pseudo-random string and hashing algorithm which could lead to predictable keys.
CVE-2021-30471	A flaw was found in PoDoFo 0.9.7. An uncontrolled recursive call in PdfNamesTree::AddToDictionary function in src/podofo/doc/PdfNamesTree.cpp can lead to a stack
CVE-2021-20178	A flaw was found in ansible module where credentials are disclosed in the console log by default and not protected by the security feature when using the bitbucket_pipeline_variable module. This flaw allows an attacker to steal bitbucket_pipeline credentials. The highest threat from this vulnerability is to confidentiality.
CVE-2021-30470	A flaw was found in PoDoFo 0.9.7. An uncontrolled recursive call among PdfTokenizer::ReadArray(), PdfTokenizer::GetNextVariant() and PdfTokenizer::ReadDataType can lead to a stack overflow.
CVE-2021-30469	A flaw was found in PoDoFo 0.9.7. An use-after-free in PoDoFo::PdfVecObjects::Clear() function can cause a denial of service via a crafted PDF file.
CVE-2020-36375	Stack overflow vulnerability in parse_equality Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.
CVE-2020-36370	Stack overflow vulnerability in parse_unary Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.
CVE-2020-10729	A flaw was found in the use of insufficiently random values in Ansible. Two random password lookups of the same length generate the equal value as the template cach for the same file since no re-evaluation happens. The highest threat from this vulnerability would be that all passwords are exposed at once for the file. This flaw affects Engine versions before 2.9.6.
CVE-2020-10774	A memory disclosure flaw was found in the Linux kernel's versions before 4.18.0-193.el8 in the sysctl subsystem when reading the /proc/sys/kernel/rh_features file. Thi a local user to read uninitialized values from the kernel memory. The highest threat from this vulnerability is to confidentiality.
CVE-2008-2544	Mounting /proc filesystem via chroot command silently mounts it in read-write mode. The user could bypass the chroot environment and gain write access to files, he w have otherwise.
CVE-2020-14327	A Server-side request forgery (SSRF) flaw was found in Ansible Tower in versions before 3.6.5 and before 3.7.2. Functionality on the Tower server is abused by supply that could lead to the server processing it. This flaw leads to the connection to internal services or the exposure of additional internal services by abusing the test featur credentials to forge HTTP/HTTPS requests from the server and retrieving the results of the response.
CVE-2021-22364	There is a denial of service vulnerability in the versions 10.1.0.126(C00E125R5P3) of HUAWEI Mate 30 and 10.1.0.152(C00E136R7P2) of HUAWEI Mate 30 (5G) . A r not verify certain parameters sufficiently and it leads to some exceptions. Successful exploit could cause a denial of service condition.
CVE-2021-27492	When opening a specially crafted 3DXML file, the application containing Datakit Software libraries CatiaV5_3dRead, CatiaV6_3dRead, Step3dRead, Ug3dReadPsr, Jt3 modules in KeyShot Versions v10.1 and prior could disclose arbitrary files to remote attackers. This is because of the passing of specially crafted content to the underly parser without taking proper restrictions such as prohibiting an external DTD.
CVE-2021-24309	The "Schedule Name" input in the Weekly Schedule WordPress plugin before 3.4.3 general options did not properly sanitize input, allowing a user to inject javascript cc <script> HTML tags and cause a stored XSS issue
CVE-2021-25932	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-founda 2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to Stored Cross-Site Scripting, since the function `validateFormInp performs improper validation checks on the input sent to the `userID` parameter. Due to this flaw an attacker could inject an arbitrary script which will be stored in the da
CVE-2021-32539	Add event in calendar function in the 101EIP system does not filter special characters in specific fields, which allows remote authenticated users to inject JavaScript an stored XSS attack.
CVE-2020-26680	In vFairs 3.3, any user logged in to a vFairs virtual conference or event can modify any other users profile information to include a cross-site scripting payload. The use by the database includes HTML tags that are intentionally rendered out onto the page, and this can be abused to perform XSS attacks.
CVE-2020-27839	A flaw was found in ceph-dashboard. The JSON Web Token (JWT) used for user authentication is stored by the frontend application in the browser's localStorage whic potentially vulnerable to attackers via XSS attacks. The highest threat from this vulnerability is to data confidentiality and integrity.

CVE Number	Description
CVE-2020-4354	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering t functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 178506.
CVE-2021-33394	Cubecart 6.4.2 allows Session Fixation. The application does not generate a new session cookie after the user is logged in. A malicious user is able to create a new se value and inject it to a victim. After the victim logs in, the injected cookie becomes valid, giving the attacker access to the user's account through the active session.
CVE-2021-27676	Centreon version 20.10.2 is affected by a cross-site scripting (XSS) vulnerability. The dep_description (Dependency Description) and dep_name (Dependency Name) p are vulnerable to stored XSS. A user has to log in and go to the Configuration > Notifications > Hosts page.
CVE-2021-31643	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization or component if.cgi - username parameter.
CVE-2019-4653	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering t functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 170964.
CVE-2021-24313	The WP Prayer WordPress plugin before 1.6.2 provides the functionality to store requested prayers/praises and list them on a WordPress website. These stored prayer requests can be listed by using the WP Prayer engine. An authenticated WordPress user with any role can fill in the form to request a prayer. The form to request praye have several fields. The 'prayer request' and 'praise request' fields do not use proper input validation and can be used to store XSS payloads.
CVE-2021-24322	The Database Backup for WordPress plugin before 2.4 did not escape the backup_recipient POST parameter in before output it back in the attribute of an HTML tag, le Stored Cross-Site Scripting issue.
CVE-2021-24334	The Instant Images – One Click Unsplash Uploads WordPress plugin before 4.4.0.1 did not properly validate and sanitise its unsplash_download_w and unsplash_dow parameter settings (/wp-admin/upload.php?page=instant-images), only validating them client side before saving them, leading to a Stored Cross-Site Scripting issue.
CVE-2020-26693	A stored cross-site scripting (XSS) vulnerability was discovered in pfSense 2.4.5-p1 which allows an authenticated attacker to execute arbitrary web scripts via exploita load_balancer_monitor.php function.
CVE-2021-29252	RSA Archer before 6.9 SP1 P1 (6.9.1.1) contains a stored XSS vulnerability. A remote authenticated malicious Archer user with access to modify link name fields could exploit this vulnerability to execute code in a victim's browser.
CVE-2020-26669	A stored cross-site scripting (XSS) vulnerability was discovered in BigTree CMS 4.4.10 and earlier which allows an authenticated attacker to execute arbitrary web scrip via the page content to site/index.php/admin/pages/update.
CVE-2021-24329	The WP Super Cache WordPress plugin before 1.7.3 did not properly sanitise its wp_cache_location parameter in its settings, which could lead to a Stored Cross-Site S issue.
CVE-2021-24319	The Bello - Directory & Listing WordPress theme before 1.6.0 did not properly sanitise its post_excerpt parameter before outputting it back in the shop/my-account/bello endpoint/ page, leading to a Cross-Site Scripting issue
CVE-2021-32540	Add announcement function in the 101EIP system does not filter special characters, which allows authenticated users to inject JavaScript and perform a stored XSS att
CVE-2020-25634	A flaw was found in Red Hat 3scale's API docs URL, where it is accessible without credentials. This flaw allows an attacker to view sensitive information or modify serv Versions before 3scale-2.10.0-ER1 are affected.
CVE-2021-32541	The CTS Web transaction system related to authentication and session management is implemented incorrectly, which allows remote unauthenticated attackers can se number of valid usernames, and force those logged-in account to log out, causing the user to be unable to access the services
CVE-2021-20585	IBM Security Verify Access 20.07 could disclose sensitive information in HTTP server headers that could be used in further attacks against the system. IBM X-Force ID
CVE-2021-28170	In the Jakarta Expression Language implementation 3.0.3 and earlier, a bug in the ELParserTokenManager enables invalid EL expressions to be evaluated as if they w
CVE-2021-23388	The package forms before 1.2.1, from 1.3.0 and before 1.3.2 are vulnerable to Regular Expression Denial of Service (ReDoS) via email validation.

CVE Number	Description
CVE-2021-20201	A flaw was found in spice in versions before 0.14.92. A DoS tool might make it easier for remote attackers to cause a denial of service (CPU consumption) by performir renegotiations within a single connection.
CVE-2021-22362	There is an out of bounds write vulnerability in some Huawei products. An attacker can exploit this vulnerability by sending crafted data in the packet to the target devic insufficient validation of message, successful exploit can cause certain service abnormal.Affected product versions include:CloudEngine 12800 versions V200R002C50SPC800,V200R003C00SPC810,V200R005C00SPC800,V200R005C10SPC800,V200R019C00SPC800,V200R019C10SPC800;CloudEngine 5800 vers V200R002C50SPC800,V200R003C00SPC810,V200R005C00SPC800,V200R005C10SPC800,V200R019C00SPC800,V200R019C10SPC800@;CloudEngine 6800 ve V200R002C50SPC800,V200R003C00SPC810,V200R005C00SPC800,V200R005C10SPC800,V200R005C20SPC800,V200R019C00SPC800,V200R019C10SPC800 7800 versions V200R002C50SPC800,V200R003C00SPC810,V200R005C00SPC800,V200R005C10SPC800,V200R019C00SPC800,V200R019C10SPC800.
CVE-2021-3424	A flaw was found in keycloak as shipped in Red Hat Single Sign-On 7.4 where IDN homograph attacks are possible. A malicious user can register himself with a name registered and trick admin to grant him extra privileges.
CVE-2021-32646	Roomer is a discord bot cog (extension) which provides automatic voice channel generation as well as private voice and text channels. A vulnerability has been discove discord users to get the ``manage channel`` permissions in a private VC they have joined. This allowed them to make changes to or delete the voice channel they have The exploit does not allow access or control to any other channels in the server. Upgrade to version 1.0.1 for a patched version of the cog. As a workaround you may d VCs in your guild(server) or unload the roomer cog to render the exploit unusable.
CVE-2018-16496	In Versa Director, the un-authentication request found.
CVE-2021-29253	The Tableau integration in RSA Archer 6.4 P1 (6.4.0.1) through 6.9 P2 (6.9.0.2) is affected by an insecure credential storage vulnerability. An malicious attacker with ac Tableau workbook file may obtain access to credential information to use it in further attacks.
CVE-2021-33182	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in PDF Viewer component in Synology DiskStation Manager (DSM) before 6.2. allows remote authenticated users to read limited files via unspecified vectors.
CVE-2021-25643	An issue was discovered in Couchbase Server 5.x and 6.x before 6.5.2 and 6.6.x before 6.6.2. Internal users with administrator privileges, @cbq-engine-cbauth and @ cbauth, leak credentials in cleartext in the indexer.log file when they make a /listCreateTokens, /listRebalanceTokens, or /listMetadataTokens call.
CVE-2021-22360	There is a resource management error vulnerability in the verisions V500R001C60SPC500, V500R005C00SPC100, V500R005C00SPC200 of USG9500. An authentic attacker needs to perform specific operations to exploit the vulnerability on the affected device. Due to improper resource management of the function, the vulnerability exploited to cause service abnormal on affected devices.
CVE-2021-28652	An issue was discovered in Squid before 4.15 and 5.x before 5.0.6. Due to incorrect parser validation, it allows a Denial of Service attack against the Cache Manager A allows a trusted client to trigger memory leaks that. over time, lead to a Denial of Service via an unspecified short query string. This attack is limited to clients with Cach API access privilege.
CVE-2021-33469	COVID19 Testing Management System 1.0 is vulnerable to Cross Site Scripting (XSS) via the "Admin name" parameter.
CVE-2020-27377	A cross-site scripting (XSS) vulnerability was discovered in the Administrator panel on the 'Setting News' module on CMS Made Simple 2.2.14 which allows an attacker arbitrary web scripts.
CVE-2021-24330	The Funnel Builder by CartFlows – Create High Converting Sales Funnels For WordPress plugin before 1.6.13 did not sanitise its facebook_pixel_id and google_analyt settings, allowing high privilege users to set XSS payload in them, which will either be executed on pages generated by the plugin, or the whole website depending on t used.
CVE-2021-24310	The Photo Gallery by 10Web - Mobile-Friendly Image Gallery WordPress plugin before 1.5.67 did not properly sanitise the gallery title, allowing high privilege users to c with XSS payload in it, which will be triggered when another user will view the gallery list or the affected gallery in the admin dashboard. This is due to an incomplete fix 2019-16117
CVE-2021-24331	The Smooth Scroll Page Up/Down Buttons WordPress plugin before 1.4 did not properly sanitise and validate its settings, such as psb_distance, psb_buttonsize, psb_s validating them client side. This could allow high privilege users (such as admin) to set XSS payloads in them
CVE-2020-18230	Cross Site Scripting (XSS) in PHPMyWind v5.5 allows remote attackers to execute arbitrary code by injecting scripts into the parameter "$cfg_switchshow" of compone /admin/web_config.php".
CVE-2020-18229	Cross Site Scripting (XSS) in PHPMyWind v5.5 allows remote attackers to execute arbitrary code by injecting scripts into the parameter "$cfg_copyright" of component /admin/web_config.php".
CVE-2021-32542	The parameters of the specific functions in the CTS Web trading system do not filter special characters, which allows unauthenticated attackers can remotely perform r and obtain the users' connection token that triggered the attack.

CVE Number	Description
CVE-2021-3425	A flaw was found in the AMQ Broker that discloses JDBC encrypted usernames and passwords when provided in the AMQ Broker application logfile when using the jdb persistence functionality. Versions shipped in Red Hat AMQ 7 are vulnerable.
CVE-2020-35505	A NULL pointer dereference flaw was found in the am53c974 SCSI host bus adapter emulation of QEMU in versions before 6.0.0. This issue occurs while handling the Transfer' command. This flaw allows a privileged guest user to crash the QEMU process on the host, resulting in a denial of service. The highest threat from this vulner system availability.
CVE-2021-20177	A flaw was found in the Linux kernel's implementation of string matching within a packet. A privileged user (with root or CAP_NET_ADMIN) when inserting iptables rule a rule which can panic the system. Kernel before kernel 5.5-rc1 is affected.
CVE-2020-10697	A flaw was found in Ansible Tower when running Openshift. Tower runs a memcached, which is accessed via TCP. An attacker can take advantage of writing a playboo this cache, causing a denial of service attack. This attack would not completely stop the service, but in the worst-case scenario, it can reduce the Tower performance, f memcached is designed. Theoretically, more sophisticated attacks can be performed by manipulating and crafting the cache, as Tower relies on memcached as a plac setting values. Confidential and sensitive data stored in memcached should not be pulled, as this information is encrypted. This flaw affects Ansible Tower versions bef Ansible Tower versions before 3.5.6 and Ansible Tower versions before 3.4.6.
CVE-2020-1729	A flaw was found in SmallRye's API through version 1.6.1. The API can allow other code running within the application server to potentially obtain the ClassLoader, byp permissions checks that should have been applied. The largest threat from this vulnerability is a threat to data confidentiality. This is fixed in SmallRye 1.6.2
CVE-2021-32657	Nextcloud Server is a Nextcloud package that handles data storage. In versions of Nextcloud Server prior to 10.0.11, 20.0.10, and 21.0.2, a malicious user may be able user administration page. This would disallow administrators to administrate users on the Nextcloud instance. The vulnerability is fixed in versions 19.0.11, 20.0.10, and workaround, administrators can use the OCC command line tool to administrate the Nextcloud users.
CVE-2020-27831	A flaw was found in Red Hat Quay, where it does not properly protect the authorization token when authorizing email addresses for repository email notifications. This f an attacker to add email addresses they do not own to repository notifications.
CVE-2021-22358	There is an insufficient input validation vulnerability in FusionCompute 8.0.0. Due to the input validation is insufficient, an attacker can exploit this vulnerability to upload the device. Successful exploit may cause the service abnormal.
CVE-2019-4722	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain sensitive information via a stack trace due to mishandling of certain error conditions. IBM X 172128.
CVE-2021-20306	A flaw was found in the BPMN editor in version jBPM 7.51.0.Final. Any authenticated user from any project can see the name of Ruleflow Groups from other projects, c user not having access to those projects. The highest threat from this vulnerability is to confidentiality.
CVE-2020-26679	vFairs 3.3 is affected by Insecure Permissions. Any user logged in to a vFairs virtual conference or event can modify any other users profile information or profile pictur receiving any user's unique identification number and their own, an HTTP POST request can be made update their profile description or supply a new profile image. Th potential cross-site scripting attacks on any user, or upload malicious PHP webshells as "profile pictures." The user IDs can be easily determined by other responses fr for an event or chat room.
CVE-2020-25724	A flaw was found in RESTEasy, where an incorrect response to an HTTP request is provided. This flaw allows an attacker to gain access to privileged information. The threat from this vulnerability is to confidentiality and integrity. Versions before resteasy 2.0.0.Alpha3 are affected.
CVE-2021-33586	InspIRCd 3.8.0 through 3.9.x before 3.10.0 allows any user (able to connect to the server) to access recently deallocated memory, aka the "malformed PONG" issue.
CVE-2020-27826	A flaw was found in Keycloak before version 12.0.0 where it is possible to update the user's metadata attributes using Account REST API. This flaw allows an attacker own NameID attribute to impersonate the admin user for any particular application.
CVE-2021-22747	Improper Check for Unusual or Exceptional Conditions vulnerability exists in Triconex Model 3009 MP installed on Tricon V11.3.x systems that could cause module res TCM receives malformed TriStation packets while the write-protect keyswitch is in the program position. This CVE ID is unique from CVE-2021-22742, CVE-2021-2274 2021-22745, and CVE-2021-22746.
CVE-2021-22745	Improper Check for Unusual or Exceptional Conditions vulnerability exists in Triconex Model 3009 MP installed on Tricon V11.3.x systems that could cause module res TCM receives malformed TriStation packets while the write-protect keyswitch is in the program position. This CVE ID is unique from CVE-2021-22742, CVE-2021-2274 2021-22746, and CVE-2021-22747.
CVE-2021-22746	Improper Check for Unusual or Exceptional Conditions vulnerability exists in Triconex Model 3009 MP installed on Tricon V11.3.x systems that could cause module res TCM receives malformed TriStation packets while the write-protect keyswitch is in the program position. This CVE ID is unique from CVE-2021-22742, CVE-2021-2274 2021-22745, and CVE-2021-22747.
CVE-2021-22744	Improper Check for Unusual or Exceptional Conditions vulnerability exists in Triconex Model 3009 MP installed on Tricon V11.3.x systems that could cause module res TCM receives malformed TriStation packets while the write-protect keyswitch is in the program position. This CVE ID is unique from CVE-2021-22742, CVE-2021-2274 2021-22746, and CVE-2021-22747.

CVE Number	Description
CVE-2021-22742	Improper Check for Unusual or Exceptional Conditions vulnerability exists in Triconex Model 3009 MP installed on Tricon V11.3.x systems that could cause module res TCM receives malformed TriStation packets while the write-protect keyswitch is in the program position.
CVE-2021-22743	Improper Check for Unusual or Exceptional Conditions vulnerability exists in Triconex TCM 4351B installed on Tricon V11.3.x systems that could cause module reset w receives malformed TriStation packets while the write-protect keyswitch is in the program position.
CVE-2021-32655	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.11, 20.0.10, and 21.0.2, an attacker is able to convert a Files Drop link to a share. This causes an issue on the UI side of the sharing user. When the sharing user opens the sharing panel and tries to remove the "Create" privileges of this unexp Nextcloud server would silently grant the share read privileges. The vulnerability is patched in versions 19.0.11, 20.0.10 and 21.0.2. No workarounds are known to exist
CVE-2020-14329	A data exposure flaw was found in Ansible Tower in versions before 3.7.2, where sensitive data can be exposed from the /api/v2/labels/ endpoint. This flaw allows user organizations in the system to retrieve any label from the organization and also disclose organization names. The highest threat from this vulnerability is to confidentiali
CVE-2021-31153	please before 0.4 allows a local unprivileged attacker to gain knowledge about the existence of files or directories in privileged locations via the search_path function, th option, or the -d option.
CVE-2021-20575	IBM Security Verify Access 20.07 allows web pages to be stored locally which can be read by another user on the system. X-Force ID: 199278.
CVE-2020-1702	A malicious container image can consume an unbounded amount of memory when being pulled to a container runtime host, such as Red Hat Enterprise Linux using po OpenShift Container Platform. An attacker can use this flaw to trick a user, with privileges to pull container images, into crashing the process responsible for pulling the flaw affects containers-image versions before 5.2.0.
CVE-2020-14328	A flaw was found in Ansible Tower in versions before 3.7.2. A Server Side Request Forgery flaw can be abused by supplying a URL which could lead to the server proc connecting to internal services or exposing additional internal services and more particularly retrieving full details in case of error. The highest threat from this vulnerabi confidentiality.
CVE-2021-20239	A flaw was found in the Linux kernel in versions before 5.4.92 in the BPF protocol. This flaw allows an attacker with a local account to leak information about kernel inte addresses. The highest threat from this vulnerability is to confidentiality.
CVE-2020-10698	A flaw was found in Ansible Tower when running jobs. This flaw allows an attacker to access the stdout of the executed jobs which are run from other organizations. So data can be disclosed. However, critical data should not be disclosed, as it should be protected by the no_log flag when debugging is enabled. This flaw affects Ansible versions before 3.6.4, Ansible Tower versions before 3.5.6 and Ansible Tower versions before 3.4.6.
CVE-2021-32651	OneDev is a development operations platform. If the LDAP external authentication mechanism is enabled in OneDev versions 4.4.1 and prior, an attacker can manipula search filter to send forged queries to the application and explore the LDAP tree using Blind LDAP Injection techniques. The specific payload depends on how the User Filter property is configured in OneDev. This issue was fixed in version 4.4.2.
CVE-2021-32653	Nextcloud Server is a Nextcloud package that handles data storage. Nextcloud Server versions prior to 19.0.11, 20.0.10, or 21.0.2 send user IDs to the lookup server e user has no fields set to published. The vulnerability is patched in versions 19.0.11, 20.0.10, and 21.0.2; no workarounds outside the updates are known to exist.
CVE-2008-3523	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA
CVE-2008-5509	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs:CVE-2008-5508. Reason: This candidate is a duplicate of CVE-2008-5508. Notes: All CVE u reference CVE-2008-5508 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage
CVE-2008-5085	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA
CVE-2008-5084	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA
CVE-2020-15440	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15438	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15442	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none

CVE Number	Description
CVE-2020-15441	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15455	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15465	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15464	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15463	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15462	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15461	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15460	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15459	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15458	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15457	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15456	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15454	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15443	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15453	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15452	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15451	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15450	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15449	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none

CVE Number	Description
CVE-2020-15448	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15447	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15446	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15445	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15444	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none
CVE-2020-15439	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with vulnerability during 2020. Notes: none