SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 22 September 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-2021-33690	Server-Side Request Forgery (SSRF) vulnerability has been detected in the SAP NetWeaver Development Infrastructure Component Build Service versions - 7.11, 7.20, 7.30, 7.31, 7.40, 7.50The SAP NetWeaver Development Infrastructure Component Build Service allows a threat actor who has access to the server to perform proxy attacks on server by sending crafted queries. Due to this, the threat actor could completely compromise sensitive data residing on the Server and impact its availability.Note: The impact of this vulnerability depends on whether SAP NetWeaver Development Infrastructure (NWDI) runs on the intranet or internet. The CVSS score reflects the impact considering the worst-case scenario that it runs on the internet.	9.9	More Details
CVE-2020-12083	An elevated privileges issue related to Spring MVC calls impacts Code Insight v7.x releases up to and including 2020 R1 (7.11.0-64).	9.9	More Details
CVE-2021-3751	libmobi is vulnerable to Out-of-bounds Write	9.8	More Details
CVE-2021-41326	In MISP before 2.4.148, app/Lib/Export/OpendataExport.php mishandles parameter data that is used in a shell_exec call.	9.8	More Details
CVE-2021-38647	Open Management Infrastructure Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-40669	SQL Injection vulnerability exists in Wuzhi CMS 4.1.0 via the keywords parameter under the coreframe/app/promote/admin/index.php file.	9.8	More Details
CVE-2021-40670	SQL Injection vulnerability exists in Wuzhi CMS 4.1.0 via the keywords iparameter under the /coreframe/app/order/admin/card.php file.	9.8	More Details
CVE-2021-1976	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2021-41303	Apache Shiro before 1.8.0, when using Apache Shiro with Spring Boot, a specially crafted HTTP request may cause an authentication bypass. Users should update to Apache Shiro 1.8.0.	9.8	More Details
CVE-2021-41317	XSS Hunter Express before 2021-09-17 does not properly enforce authentication requirements for paths.	9.8	More Details
CVE-2021-41392	static/main-preload.js in Boost Note through 0.22.0 allows remote command execution. A remote attacker may send a crafted IPC message to the exposed vulnerable ipcRenderer IPC interface, which invokes the dangerous openExternal Electron API.	9.8	More Details
CVE-2020-14124	There is a buffer overflow in librsa.so called by getwifipwdurl interface, resulting in code execution on Xiaomi router AX3600 with ROM version =rom< 1.1.12.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41393	Teleport before 4.4.11, 5.x before 5.2.4, 6.x before 6.2.12, and 7.x before 7.1.1 allows forgery of SSH host certificates in some situations.	9.8	More Details
CVE-2021-24741	The Support Board WordPress plugin before 3.3.4 does not escape multiple POST parameters (such as status_code, department, user_id, conversation_id, conversation_status_code, and recipient_id) before using them in SQL statements, leading to SQL injections which are exploitable by unauthenticated users.	9.8	More Details
CVE-2021-40674	An SQL injection vulnerability exists in Wuzhi CMS v4.1.0 via the KeyValue parameter in coreframe/app/order/admin/index.php.	9.8	More Details
CVE-2021-31917	A flaw was found in Red Hat DataGrid 8.x (8.0.0, 8.0.1, 8.1.0 and 8.1.1) and Infinispan (10.0.0 through 12.0.0). An attacker could bypass authentication on all REST endpoints when DIGEST is used as the authentication method. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	9.8	More Details
CVE-2021-0869	In GetTimeStampAndPkt of DumpstateDevice.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-179620905 References: N/A	9.8	More Details
CVE-2021-28960	Zoho ManageEngine Desktop Central before build 10.0.683 allows unauthenticated command injection due to improper handling of an input command in on-demand operations.	9.8	More Details
CVE-2021-27341	OpenSIS Community Edition version <= 7.6 is affected by a local file inclusion vulnerability in DownloadWindow.php via the "filename" parameter.	9.8	More Details
CVE-2021-39275	ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.	9.8	More Details
CVE-2020-14119	There is command injection in the addMeshNode interface of xqnetwork.lua, which leads to command execution under administrator authority on Xiaomi router AX3600 with rom versionrom< 1.1.12	9.8	More Details
CVE-2021-37909	WriteRegistry function in TSSServiSign component does not filter and verify users' input, remote attackers can rewrite to the registry without permissions thus perform hijack attacks to execute arbitrary code.	9.8	More Details
CVE-2021-3797	hestiacp is vulnerable to Use of Wrong Operator in String Comparison	9.8	More Details
CVE-2020-21121	Pligg CMS 2.0.2 contains a time-based SQL injection vulnerability via the $recordIDValue parameter in the admin_update_module_widgets.php file.	9.8	More Details
CVE-2020-21124	UReport 2.2.9 allows attackers to execute arbitrary code due to a lack of access control to the designer page.	9.8	More Details
CVE-2020-21125	An arbitrary file creation vulnerability in UReport 2.2.9 allows attackers to execute arbitrary code.	9.8	More Details
CVE-2020-21127	MetInfo 7.0.0 contains a SQL injection vulnerability via admin/?n=logs&c=index&a=dodel.	9.8	More Details
CVE-2021-39392	The management tool in MyLittleBackup up to and including 1.7 allows remote attackers to execute arbitrary code because machineKey is hardcoded (the same for all customers' installations) in web.config, and can be used to send serialized ASP code.	9.8	More Details
CVE-2021-40881	An issue in the BAT file parameters of PublicCMS v4.0 allows attackers to execute arbitrary code.	9.8	More Details
CVE-2021-37424	ManageEngine ADSelfService Plus before 6112 is vulnerable to domain user account takeover.	9.8	More Details
CVE-2021-37912	The HGiga OAKlouds mobile portal does not filter special characters of the Ethernet number parameter of the network interface card setting page. Remote attackers can use this vulnerability to perform command injection and execute arbitrary commands in the system without logging in.	9.8	More Details
CVE-2021-37913	The HGiga OAKlouds mobile portal does not filter special characters of the IPv6 Gateway parameter of the network interface card setting page. Remote attackers can use this vulnerability to perform command injection and execute arbitrary commands in the system without logging in.	9.8	More Details
CVE-2020-21322	An arbitrary file upload vulnerability in Feehi CMS v2.0.8 and below allows attackers to execute arbitrary code via a crafted PHP file.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33044	The identity authentication bypass vulnerability found in some Dahua products during the login process. Attackers can bypass device identity authentication by constructing malicious data packets.	9.8	More Details
CVE-2021-33045	The identity authentication bypass vulnerability found in some Dahua products during the login process. Attackers can bypass device identity authentication by constructing malicious data packets.	9.8	More Details
CVE-2021-38412	Properly formatted POST requests to multiple resources on the HTTP and HTTPS web servers of the Digi PortServer TS 16 Rack device do not require authentication or authentication tokens. This vulnerability could allow an attacker to enable the SNMP service and manipulate the community strings to achieve further control in.	9.6	More Details
CVE-2021-20790	Improper control of program execution vulnerability in RevoWorks Browser 2.1.230 and earlier allows an attacker to execute an arbitrary command or code via unspecified vectors.	9.6	More Details
CVE-2021-20791	Improper access control vulnerability in RevoWorks Browser 2.1.230 and earlier allows an attacker to bypass access restriction and to exchange unauthorized files between the local environment and the isolated environment or settings of the web browser via unspecified vectors.	9.3	More Details
CVE-2021-33695	Potentially, SAP Cloud Connector, version - 2.0 communication with the backend is accepted without sufficient validation of the certificate.	9.1	More Details
CVE-2021-24638	The OMGF WordPress plugin before 4.5.4 does not escape or validate the handle parameter of the REST API, which allows unauthenticated users to perform path traversal and overwrite arbitrary CSS file with Google Fonts CSS, or download fonts uploaded on Google Fonts website.	9.1	More Details
CVE-2021-33701	DMIS Mobile Plug-In or SAP S/4HANA, versions - DMIS 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 710, 2011_1_731, 710, 2011_1_752, 2020, SAPSCORE 125, S4CORE 102, 102, 103, 104, 105, allows an attacker with access to highly privileged account to execute manipulated query in NDZT tool to gain access to Superuser account, leading to SQL Injection vulnerability, that highly impacts systems Confidentiality, Integrity and Availability.	9.1	More Details
CVE-2021-40438	A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-39537	An issue was discovered in ncurses through v6.2-1. _nc_captoinfo in captoinfo.c has a heap-based buffer overflow.	8.8	More Details
CVE-2021-33704	The Service Layer of SAP Business One, version - 10.0, allows an authenticated attacker to invoke certain functions that would otherwise be restricted to specific users. For an attacker to discover the vulnerable function, no in-depth system knowledge is required. Once exploited via Network stack, the attacker may be able to read, modify or delete restricted data. The impact is that missing authorization can result of abuse of functionality usually restricted to specific users.	8.8	More Details
CVE-2020-21598	libde265 v1.0.4 contains a heap buffer overflow in the ff_hevc_put_unweighted_pred_8_sse function, which can be exploited via a crafted a file.	8.8	More Details
CVE-2021-41387	seatd-launch in seatd 0.6.x before 0.6.2 allows privilege escalation because it uses execlp and may be installed setuid root.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40444	Microsoft is investigating reports of a remote code execution vulnerability in MSHTML that affects Microsoft Windows. Microsoft is aware of targeted attacks that attempt to exploit this vulnerability by using specially-crafted Microsoft Office documents. An attacker could craft a malicious ActiveX control to be used by a Microsoft Office document that hosts the browser rendering engine. The attacker would then have to convince the user to open the malicious document. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Microsoft Defender Antivirus and Microsoft Defender for Endpoint both provide detection and protections for the known vulnerability. Customers should keep antimalware products up to date. Customers who utilize automatic updates do not need to take additional action. Enterprise customers who manage updates should select the detection build 1.349.22.0 or newer and deploy it across their environments. Microsoft Defender for Endpoint alerts will be displayed as: “Suspicious Cpl File Execution”. Upon completion of this investigation, Microsoft will take the appropriate action to help protect our customers. This may include providing a security update through our monthly release process or providing an out-of-cycle security update, depending on customer needs. Please see the Mitigations and Workaround sections for important information about steps you can take to protect your system from this vulnerability. UPDATE September 14, 2021: Microsoft has released security updates to address this vulnerability. Please see the Security Updates table for the applicable update for your system. We recommend that you install these updates immediately. Please see the FAQ for important information about which updates are applicable to your system.	8.8	More Details
CVE-2021-38092	Integer Overflow vulnerability in function filter_prewitt in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	8.8	More Details
CVE-2021-39525	An issue was discovered in libredwg through v0.10.1.3751. bit_read_fixed() in bits.c has a heap-based buffer overflow.	8.8	More Details
CVE-2020-21548	Libsixel 1.8.3 contains a heap-based buffer overflow in the sixel_encode_highcolor function in tosixel.c.	8.8	More Details
CVE-2020-19151	Command Injection in Jfinal CMS v4.7.1 and earlier allows remote attackers to execute arbitrary code by uploading a malicious HTML template file via the component 'jfinal_cms/admin/filemanager/list'.	8.8	More Details
CVE-2021-38093	Integer Overflow vulnerability in function filter_robert in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	8.8	More Details
CVE-2021-38094	Integer Overflow vulnerability in function filter_sobel in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	8.8	More Details
CVE-2020-21547	Libsixel 1.8.2 contains a heap-based buffer overflow in the dither_func_fs function in tosixel.c.	8.8	More Details
CVE-2021-40845	The web part of Zenitel AlphaCom XE Audio Server through 11.2.3.10, called AlphaWeb XE, does not restrict file upload in the Custom Scripts section at php/index.php. Neither the content nor extension of the uploaded files is checked, allowing execution of PHP code under the /cmd directory.	8.8	More Details
CVE-2021-25741	A security issue was discovered in Kubernetes where a user may be able to create a container with subpath volume mounts to access files & directories outside of the volume, including on the host filesystem.	8.8	More Details
CVE-2021-24404	The options.php file of the WP-Board WordPress plugin through 1.1 beta accepts a postid parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. This is a time based SQLI and in the same function vulnerable parameter is passed twice so if we pass time as 5 seconds it takes 10 seconds to return since the query ran twice.	8.8	More Details
CVE-2021-39536	An issue was discovered in libxsmm through v1.16.1-93. The JIT code has a heap-based buffer overflow.	8.8	More Details
CVE-2021-32265	An issue was discovered in Bento4 through v1.6.0-637. A global-buffer-overflow exists in the function AP4_MemoryByteStream::WritePartial() located in Ap4ByteStream.cpp. It allows an attacker to cause code execution or information disclosure.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20898	Integer Overflow vulnerability in function filter16_prewitt in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	8.8	More Details
CVE-2021-41314	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.	8.8	More Details
CVE-2020-20896	An issue was discovered in function latm_write_packet in libavformat/latmenc.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts due to a Null pointer dereference.	8.8	More Details
CVE-2020-20892	An issue was discovered in function filter_frame in libavfilter/vf_lenscorrection.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts due to a division by zero.	8.8	More Details
CVE-2021-41315	The Device42 Remote Collector before 17.05.01 does not sanitize user input in its SNMP Connectivity utility. This allows an authenticated attacker (with access to the console application) to execute arbitrary OS commands and escalate privileges.	8.8	More Details
CVE-2021-39522	An issue was discovered in libredwg through v0.10.1.3751. bit_wcs2len() in bits.c has a heap-based buffer overflow.	8.8	More Details
CVE-2021-33698	SAP Business One, version - 10.0, allows an attacker with business authorization to upload any files (including script files) without the proper file format validation.	8.8	More Details
CVE-2021-24606	The Availability Calendar WordPress plugin before 1.2.1 does not escape the category attribute from its shortcode before using it in a SQL statement, leading to a SQL Injection issue, which can be exploited by any user able to add shortcode to posts/pages, such as contributor+	8.8	More Details
CVE-2020-19155	Improper Access Control in Jfinal CMS v4.7.1 and earlier allows remote attackers to obtain sensitive information and/or execute arbitrary code via the 'FileManager.rename()' function in the component 'modules/filemanager/FileManagerController.java'.	8.8	More Details
CVE-2021-38091	Integer Overflow vulnerability in function filter16_sobel in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	8.8	More Details
CVE-2021-37741	ManageEngine ADManager Plus before 7111 has Pre-authentication RCE vulnerabilities.	8.8	More Details
CVE-2021-39531	An issue was discovered in libslax through v0.22.1. slaxLexer() in slaxlexer.c has a stack-based buffer overflow.	8.8	More Details
CVE-2021-39209	GLPI is a free Asset and IT management software package. In versions prior to 9.5.6, a user who is logged in to GLPI can bypass Cross-Site Request Forgery (CSRF) protection in many places. This could allow a malicious actor to perform many actions on GLPI. This issue is fixed in version 9.5.6. There are no workarounds aside from upgrading.	8.8	More Details
CVE-2021-39530	An issue was discovered in libredwg through v0.10.1.3751. bit_wcs2nlen() in bits.c has a heap-based buffer overflow.	8.8	More Details
CVE-2021-22148	Elastic Enterprise Search App Search versions before 7.14.0 was vulnerable to an issue where API keys were not bound to the same engines as their creator. This could lead to a less privileged user gaining access to unauthorized engines.	8.8	More Details
CVE-2021-22149	Elastic Enterprise Search App Search versions before 7.14.0 are vulnerable to an issue where API keys were missing authorization via an alternate route. Using this vulnerability, an authenticated attacker could utilize API keys belonging to higher privileged users.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19159	Cross Site Request Forgery (CSRF) in LaikeTui v3 allows remote attackers to execute arbitrary code via the component '/index.php?module=member&action=add'.	8.8	More Details
CVE-2021-39534	An issue was discovered in libslax through v0.22.1. slaxIsCommentStart() in slaxlexer.c has a heap-based buffer overflow.	8.8	More Details
CVE-2020-19551	Blacklist bypass issue exists in WUZHI CMS up to and including 4.1.0 in common.func.php, which when uploaded can cause remote code executiong.	8.8	More Details
CVE-2020-21126	MetInfo 7.0.0 contains a Cross-Site Request Forgery (CSRF) via admin/?n=admin&c=index&a=doSaveInfo.	8.8	More Details
CVE-2021-36954	Windows Bind Filter Driver Elevation of Privilege Vulnerability	8.8	More Details
CVE-2021-32294	An issue was discovered in libgig through 20200507. A heap-buffer-overflow exists in the function RIFF::List::GetSubList located in RIFF.cpp. It allows an attacker to cause code Execution.	8.8	More Details
CVE-2021-40862	HashiCorp Terraform Enterprise up to v202108-1 contained an API endpoint that erroneously disclosed a sensitive URL to authenticated parties, which could be used for privilege escalation or unauthorized modification of a Terraform configuration. Fixed in v202109-1.	8.8	More Details
CVE-2021-39533	An issue was discovered in libslax through v0.22.1. slaxLexer() in slaxlexer.c has a heap-based buffer overflow.	8.8	More Details
CVE-2021-32297	An issue was discovered in LIEF through 0.11.4. A heap-buffer-overflow exists in the function main located in pe_reader.c. It allows an attacker to cause code Execution.	8.8	More Details
CVE-2021-39230	Butter is a system usability utility. Due to a kernel error the JPNS kernel is being discontinued. Affected users are recommend to update to the Trinity kernel. There are no workarounds.	8.8	More Details
CVE-2021-40965	A Cross-Site Request Forgery (CSRF) vulnerability exists in TinyFileManager all version up to and including 2.4.6 that allows attackers to upload files and run OS commands by inducing the Administrator user to browse a URL controlled by an attacker.	8.8	More Details
CVE-2021-32298	An issue was discovered in libiff through 20190123. A global-buffer-overflow exists in the function IFF_errorId located in error.c. It allows an attacker to cause code Execution.	8.8	More Details
CVE-2021-39528	An issue was discovered in libredwg through v0.10.1.3751. dwg_free_MATERIAL_private() in dwg.spec has a double free.	8.8	More Details
CVE-2021-36965	Windows WLAN AutoConfig Service Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-39527	An issue was discovered in libredwg through v0.10.1.3751. appinfo_private() in decode.c has a heap-based buffer overflow.	8.8	More Details
CVE-2020-20891	Buffer Overflow vulnerability in function config_input in libavfilter/vf_gblur.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	8.8	More Details
CVE-2021-38090	Integer Overflow vulnerability in function filter16_roberts in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41086	jsuites is an open source collection of common required javascript web components. In affected versions users are subject to cross site scripting (XSS) attacks via clipboard content. jsuites is vulnerable to DOM based XSS if the user can be tricked into copying _anything_ from a malicious and pasting it into the html editor. This is because a part of the clipboard content is directly written to `innerHTML` allowing for javascript injection and thus XSS. Users are advised to update to version 4.9.11 to resolve.	8.7	More Details
CVE-2021-41084	http4s is an open source scala interface for HTTP. In affected versions http4s is vulnerable to response-splitting or request-splitting attacks when untrusted user input is used to create any of the following fields: Header names (`Header.name`å), Header values (`Header.value`), Status reason phrases (`Status.reason`), URI paths (`Uri.Path`), URI authority registered names (`URI.RegName`) (through 0.21). This issue has been resolved in versions 0.21.30, 0.22.5, 0.23.4, and 1.0.0-M27 perform the following. As a matter of practice http4s services and client applications should sanitize any user input in the aforementioned fields before returning a request or response to the backend. The carriage return, newline, and null characters are the most threatening.	8.7	More Details
CVE-2021-23442	This affects all versions of package @cookiex/deep. The global proto object can be polluted using the __proto__ object.	8.6	More Details
CVE-2021-40825	nLight ECLYPSE (nECY) system Controllers running software prior to 1.17.21245.754 contain a default key vulnerability. The nECY does not force a change to the key upon the initial configuration of an affected device. nECY system controllers utilize an encrypted channel to secure SensorViewTM configuration and monitoring software and nECY to nECY communications. Impacted devices are at risk of exploitation. A remote attacker with IP access to an impacted device could submit lighting control commands to the nECY by leveraging the default key. A successful attack may result in the attacker gaining the ability to modify lighting conditions or gain the ability to update the software on lighting devices. The impacted key is referred to as the SensorView Password in the nECY nLight Explorer Interface and the Gateway Password in the SensorView application. An attacker cannot authenticate to or modify the configuration or software of the nECY system controller.	8.6	More Details
CVE-2021-27662	The KT-1 door controller is susceptible to replay or man-in-the-middle attacks where an attacker can record and replay TCP packets. This issue affects Johnson Controls KT-1 all versions up to and including 3.01	8.6	More Details
CVE-2021-30261	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-30260	Possible Integer overflow to buffer overflow issue can occur due to improper validation of input parameters when extscan hostlist configuration command is received in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	8.4	More Details
CVE-2021-1947	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	8.4	More Details
CVE-2021-31845	A buffer overflow vulnerability in McAfee Data Loss Prevention (DLP) Discover prior to 11.6.100 allows an attacker in the same network as the DLP Discover to execute arbitrary code through placing carefully constructed Ami Pro (.sam) files onto a machine and having DLP Discover scan it, leading to remote code execution with elevated privileges. This is caused by the destination buffer being of fixed size and incorrect checks being made on the source size.	8.4	More Details
CVE-2020-3960	VMware ESXi (6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain an out-of-bounds read vulnerability in NVMe functionality. A malicious actor with local non-administrative access to a virtual machine with a virtual NVMe controller present may be able to read privileged information contained in physical memory.	8.4	More Details
CVE-2021-1939	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	8.4	More Details
CVE-2021-31844	A buffer overflow vulnerability in McAfee Data Loss Prevention (DLP) Endpoint for Windows prior to 11.6.200 allows a local attacker to execute arbitrary code with elevated privileges through placing carefully constructed Ami Pro (.sam) files onto the local system and triggering a DLP Endpoint scan through accessing a file. This is caused by the destination buffer being of fixed size and incorrect checks being made on the source size.	8.2	More Details
CVE-2021-24639	The OMGF WordPress plugin before 4.5.4 does not enforce path validation, authorisation and CSRF checks in the omgf_ajax_empty_dir AJAX action, which allows any authenticated users to delete arbitrary files or folders on the server.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24636	The Print My Blog WordPress Plugin before 3.4.2 does not enforce nonce (CSRF) checks, which allows attackers to make logged in administrators deactivate the Print My Blog plugin and delete all saved data for that plugin by tricking them to open a malicious link	8.1	More Details
CVE-2021-41316	The Device42 Main Appliance before 17.05.01 does not sanitize user input in its Nmap Discovery utility. An attacker (with permissions to add or edit jobs run by this utility) can inject an extra argument to overwrite arbitrary files as the root user on the Remote Collector.	8.1	More Details
CVE-2021-33705	The SAP NetWeaver Portal, versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, component Iviews Editor contains a Server-Side Request Forgery (SSRF) vulnerability which allows an unauthenticated attacker to craft a malicious URL which when clicked by a user can make any type of request (e.g. POST, GET) to any internal or external server. This can result in the accessing or modification of data accessible from the Portal but will not affect its availability.	8.1	More Details
CVE-2020-19150	Improper Access Control in Jfinal CMS v4.7.1 and earlier allows remote attackers to obtain sensitive information or cause a denial of service via the 'FileManager.delete()' function in the component 'modules/filemanager/FileManagerController.java'.	8.1	More Details
CVE-2021-39214	mitmproxy is an interactive, SSL/TLS-capable intercepting proxy. In mitmproxy 7.0.2 and below, a malicious client or server is able to perform HTTP request smuggling attacks through mitmproxy. This means that a malicious client/server could smuggle a request/response through mitmproxy as part of another request/response's HTTP message body. While a smuggled request is still captured as part of another request's body, it does not appear in the request list and does not go through the usual mitmproxy event hooks, where users may have implemented custom access control checks or input sanitization. Unless one uses mitmproxy to protect an HTTP/1 service, no action is required. The vulnerability has been fixed in mitmproxy 7.0.3 and above.	8.1	More Details
CVE-2021-29831	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 204775.	8.1	More Details
CVE-2021-40847	The update process of the Circle Parental Control Service on various NETGEAR routers allows remote attackers to achieve remote code execution as root via a MitM attack. While the parental controls themselves are not enabled by default on the routers, the Circle update daemon, circled, is enabled by default. This daemon connects to Circle and NETGEAR to obtain version information and updates to the circled daemon and its filtering database. However, database updates from NETGEAR are unsigned and downloaded via cleartext HTTP. As such, an attacker with the ability to perform a MitM attack on the device can respond to circled update requests with a crafted, compressed database file, the extraction of which gives the attacker the ability to overwrite executable files with attacker-controlled code. This affects R6400v2 1.0.4.106, R6700 1.0.2.16, R6700v3 1.0.4.106, R6900 1.0.2.16, R6900P 1.3.2.134, R7000 1.0.11.123, R7000P 1.3.2.134, R7850 1.0.5.68, R7900 1.0.4.38, R8000 1.0.4.68, and RS400 1.5.0.68.	8.1	More Details
CVE-2021-26435	Windows Scripting Engine Memory Corruption Vulnerability	8.1	More Details
CVE-2021-41390	In Ericsson ECM before 18.0, it was observed that Security Provider Endpoint in the User Profile Management Section is vulnerable to CSV Injection.	8.0	More Details
CVE-2021-36967	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability	8.0	More Details
CVE-2021-41083	Dada Mail is a web-based e-mail list management system. In affected versions a bad actor could give someone a carefully crafted web page via email, SMS, etc, that - when visited, allows them control of the list control panel as if the bad actor was logged in themselves. This includes changing any mailing list password, as well as the Dada Mail Root Password - which could effectively shut out actual list owners of the mailing list and allow the bad actor complete and unfettered control of your mailing list. This vulnerability also affects profile logins. For this vulnerability to work, the target of the bad actor would need to be logged into the list control panel themselves. This CSRF vulnerability in Dada Mail affects all versions of Dada Mail v11.15.1 and below. Although we know of no known CSRF exploits that have happened in the wild, this vulnerability has been confirmed by our testing, and by a third party. Users are advised to update to version 11.16.0.	8.0	More Details
CVE-2021-27046	A Memory Corruption vulnerability for PDF files in Autodesk Navisworks 2019, 2020, 2021, 2022 may lead to code execution through maliciously crafted DLL files.	7.8	More Details
CVE-2021-27045	A maliciously crafted PDF file in Autodesk Navisworks 2019, 2020, 2021, 2022 can be forced to read beyond allocated boundaries when parsing the PDF file. This vulnerability can be exploited to execute arbitrary code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39540	An issue was discovered in pdftools through 20200714. A stack-buffer-overflow exists in the function Analyze::AnalyzePages() located in analyze.cpp. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-38300	arch/mips/net/bpf_jit.c in the Linux kernel before 5.4.10 can generate undesirable machine code when transforming unprivileged cBPF programs, allowing execution of arbitrary code within the kernel context. This occurs because conditional branches can exceed the 128 KB limit of the MIPS architecture.	7.8	More Details
CVE-2021-40155	A maliciously crafted DWG file in Autodesk Navisworks 2019, 2020, 2021, 2022 can be forced to read beyond allocated boundaries when parsing the DWG files. This vulnerability can be exploited to execute arbitrary code.	7.8	More Details
CVE-2021-40156	A maliciously crafted DWG file in Autodesk Navisworks 2019, 2020, 2021, 2022 can be forced to write beyond allocated boundaries when parsing the DWG files. This vulnerability can be exploited to execute arbitrary code.	7.8	More Details
CVE-2021-33700	SAP Business One, version - 10.0, allows a local attacker with access to the victim's browser under certain circumstances, to login as the victim without knowing his/her password. The attacker could so obtain highly sensitive information which the attacker could use to take substantial control of the vulnerable application.	7.8	More Details
CVE-2021-27044	A Out-Of-Bounds Read/Write Vulnerability in Autodesk FBX Review version 1.4.0 may lead to remote code execution through maliciously crafted DLL files or information disclosure.	7.8	More Details
CVE-2021-32268	Buffer overflow vulnerability in function gf_fprintf in os_file.c in gpac before 1.0.1 allows attackers to execute arbitrary code. The fixed version is 1.0.1.	7.8	More Details
CVE-2021-32271	An issue was discovered in gpac through 20200801. A stack-buffer-overflow exists in the function DumpRawUIConfig located in odf_dump.c. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-32272	An issue was discovered in faad2 before 2.10.0. A heap-buffer-overflow exists in the function stszin located in mp4read.c. It allows an attacker to cause Code Execution.	7.8	More Details
CVE-2021-32273	An issue was discovered in faad2 through 2.10.0. A stack-buffer-overflow exists in the function ftypin located in mp4read.c. It allows an attacker to cause Code Execution.	7.8	More Details
CVE-2021-32274	An issue was discovered in faad2 through 2.10.0. A heap-buffer-overflow exists in the function sbr_qmf_synthesis_64 located in sbr_qmf.c. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-32277	An issue was discovered in faad2 through 2.10.0. A heap-buffer-overflow exists in the function sbr_qmf_analysis_32 located in sbr_qmf.c. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-32299	An issue was discovered in pbrt through 20200627. A stack-buffer-overflow exists in the function pbrt::ParamSet::ParamSet() located in paramset.h. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-32288	An issue was discovered in heif through v3.6.2. A global-buffer-overflow exists in the function HevcDecoderConfigurationRecord::getPicHeight() located in hevcdecoderconfigrecord.cpp. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-32287	An issue was discovered in heif through v3.6.2. A global-buffer-overflow exists in the function HevcDecoderConfigurationRecord::getPicWidth() located in hevcdecoderconfigrecord.cpp. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-32286	An issue was discovered in hcxtools through 6.1.6. A global-buffer-overflow exists in the function pcapngoptionwalk located in hcxpcapngtool.c. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-32284	An issue was discovered in gravity through 0.8.1. A NULL pointer dereference exists in the function ircode_register_pop_context_protect() located in gravity_ircode.c. It allows an attacker to cause Denial of Service.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40157	A user may be tricked into opening a malicious FBX file which may exploit an Untrusted Pointer Dereference vulnerability in FBX's Review version 1.5.0 and prior causing it to run arbitrary code on the system.	7.8	More Details
CVE-2021-39561	An issue was discovered in swftools through 20200710. A stack-buffer-overflow exists in the function Gfx::opSetFillColorN() located in Gfx.cc. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-39544	An issue was discovered in sela through 20200412. file::WavFile::writeToFile() in wav_file.c has a heap-based buffer overflow.	7.8	More Details
CVE-2021-38655	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-38653	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-39546	An issue was discovered in sela through 20200412. rice::RiceDecoder::process() in rice_decoder.cpp has a heap-based buffer overflow.	7.8	More Details
CVE-2021-38406	Delta Electronic DOPSoft 2 (Version 2.00.07 and prior) lacks proper validation of user-supplied data when parsing specific project files. This could result in multiple out-of-bounds write instances. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-38648	Open Management Infrastructure Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-38646	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-38645	Open Management Infrastructure Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-38644	Microsoft MPEG-2 Video Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-38639	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-38638	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-38633	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-20037	SonicWall Global VPN Client 4.10.5 installer (32-bit and 64-bit) incorrect default file permission vulnerability leads to privilege escalation which potentially allows command execution in the host operating system. This vulnerability impacts GVC 4.10.5 installer and earlier.	7.8	More Details
CVE-2021-38630	Windows Event Tracing Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-38628	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38626	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-38625	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-36975	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-36974	Windows SMB Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-36973	Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-36968	Windows DNS Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-36966	Windows Subsystem for Linux Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-36964	Windows Event Tracing Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-36963	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-41073	loop_rw_iter in fs/io_uring.c in the Linux kernel 5.10 through 5.14.6 allows local users to gain privileges by using IORING_OP_PROVIDE_BUFFERS to trigger a free of a kernel buffer, as demonstrated by using /proc/<pid>/maps for exploitation.	7.8	More Details
CVE-2021-36955	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-36952	Visual Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-26434	Visual Studio Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-3778	vim is vulnerable to Heap-based Buffer Overflow	7.8	More Details
CVE-2021-38654	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-32281	An issue was discovered in gravity through 0.8.1. A heap-buffer-overflow exists in the function gnode_function_add_upvalue located in gravity_ast.c. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-38656	Microsoft Word Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38404	Delta Electronic DOPSoft 2 (Version 2.00.07 and prior) lacks proper validation of user-supplied data when parsing specific project files. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-21798	An exploitable return of stack variable address vulnerability exists in the JavaScript implementation of Nitro Pro PDF. A specially crafted document can cause a stack variable to go out of scope, resulting in the application dereferencing a stale pointer. This can lead to code execution under the context of the application. An attacker can convince a user to open a document to trigger the vulnerability.	7.8	More Details
CVE-2021-39550	An issue was discovered in sela through 20200412. file::SelaFile::readFromFile() in sela_file.cpp has a heap-based buffer overflow.	7.8	More Details
CVE-2021-39551	An issue was discovered in sela through 20200412. file::SelaFile::readFromFile() in sela_file.c has a heap-based buffer overflow.	7.8	More Details
CVE-2021-39552	An issue was discovered in sela through 20200412. file::WavFile::readFromFile() in wav_file.c has a heap-based buffer overflow.	7.8	More Details
CVE-2021-39558	An issue was discovered in swftools through 20200710. A stack-buffer-overflow exists in the function VectorGraphicOutputDev::drawGeneralImage() located in VectorGraphicOutputDev.cc. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-32278	An issue was discovered in faad2 through 2.10.0. A heap-buffer-overflow exists in the function lt_prediction located in lt_predict.c. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-39564	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function swf_DumpActions() located in swfaction.c. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-39569	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function OpAdvance() located in swfaction.c. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-39574	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function pool_read() located in pool.c. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-39577	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function main() located in swfdump.c. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-39579	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function string_hash() located in q.c. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-39582	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function swf_GetPlaceObject() located in swfobject.c. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-39595	An issue was discovered in swftools through 20200710. A stack-buffer-overflow exists in the function rfx_alloc() located in mem.c. It allows an attacker to cause code Execution.	7.8	More Details
CVE-2021-40447	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-38304	Improper input validation in the National Instruments NI-PAL driver in versions 20.0.0 and prior may allow a privileged user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-38671	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38402	Delta Electronic DOPSoft 2 (Version 2.00.07 and prior) lacks proper validation of user-supplied data when parsing specific project files. This could lead to a stack-based buffer overflow while trying to copy to a buffer during font string handling. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-38658	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-38667	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-38661	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-38660	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-38659	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-30137	Assyst 10 SP7.5 has authenticated XXE leading to SSRF via XML unmarshalling. The application allows users to send JSON or XML data to the server. It was possible to inject malicious XML data through several access points.	7.7	More Details
CVE-2021-38652	Microsoft SharePoint Server Spoofing Vulnerability	7.6	More Details
CVE-2021-38650	Microsoft Office Spoofing Vulnerability	7.6	More Details
CVE-2021-38651	Microsoft SharePoint Server Spoofing Vulnerability	7.6	More Details
CVE-2021-3777	nodejs-tmpl is vulnerable to Inefficient Regular Expression Complexity	7.5	More Details
CVE-2021-40690	All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfo from a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.	7.5	More Details
CVE-2021-3807	ansi-regex is vulnerable to Inefficient Regular Expression Complexity	7.5	More Details
CVE-2021-3803	nth-check is vulnerable to Inefficient Regular Expression Complexity	7.5	More Details
CVE-2021-3810	code-server is vulnerable to Inefficient Regular Expression Complexity	7.5	More Details
CVE-2021-3805	object-path is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	7.5	More Details
CVE-2020-12080	A Denial of Service vulnerability has been identified in FlexNet Publisher's lmadmin.exe version 11.16.6. A certain message protocol can be exploited to cause lmadmin to crash.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-9060	An issue was discovered in CMS Made Simple 2.2.8. It is possible to achieve unauthenticated path traversal in the CGExtensions module (in the file action.setdefaulttemplate.php) with the m1_filename parameter; and through the action.showmessage.php file, it is possible to read arbitrary file content (by using that path traversal with m1_prefname set to cg_errormsg and m1_resettodefault=1).	7.5	More Details
CVE-2020-21468	A segmentation fault in the redis-server component of Redis 5.0.7 leads to a denial of service (DOS). NOTE: the vendor cannot reproduce this issue in a released version, such as 5.0.7	7.5	More Details
CVE-2021-3804	taro is vulnerable to Inefficient Regular Expression Complexity	7.5	More Details
CVE-2021-3706	adminlte is vulnerable to Sensitive Cookie Without 'HttpOnly' Flag	7.5	More Details
CVE-2021-29825	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. IBM X-Force ID: 204470.	7.5	More Details
CVE-2021-40639	Improper access control in Jfinal CMS 5.1.0 allows attackers to access sensitive information via /classes/conf/db.properties&config=filemanager.config.js.	7.5	More Details
CVE-2021-32838	Flask-RESTX (pypi package flask-restx) is a community driven fork of Flask-RESTPlus. Flask-RESTX before version 0.5.1 is vulnerable to ReDoS (Regular Expression Denial of Service) in email_regex. This is fixed in version 0.5.1.	7.5	More Details
CVE-2021-32839	sqlparse is a non-validating SQL parser module for Python. In sqlparse versions 0.4.0 and 0.4.1 there is a regular Expression Denial of Service in sqlparse vulnerability. The regular expression may cause exponential backtracking on strings containing many repetitions of '\r\n' in SQL comments. Only the formatting feature that removes comments from SQL statements is affected by this regular expression. As a workaround don't use the sqlformat.format function with keyword strip_comments=True or the --strip-comments command line flag when using the sqlformat command line tool. The issues has been fixed in sqlparse 0.4.2.	7.5	More Details
CVE-2021-41082	Discourse is a platform for community discussion. In affected versions any private message that includes a group had its title and participating user exposed to users that do not have access to the private messages. However, access control for the private messages was not compromised as users were not able to view the posts in the leaked private message despite seeing it in their inbox. The problematic commit was reverted around 32 minutes after it was made. Users are encouraged to upgrade to the latest commit if they are running Discourse against the `tests-passed` branch.	7.5	More Details
CVE-2021-3794	vuelidate is vulnerable to Inefficient Regular Expression Complexity	7.5	More Details
CVE-2021-39229	Apprise is an open source library which allows you to send a notification to almost all of the most popular notification services available. In affected versions users who use Apprise granting them access to the IFTTT plugin (which just comes out of the box) are subject to a denial of service attack on an inefficient regular expression. The vulnerable regular expression is [here] (https://github.com/caronc/apprise/blob/0007eade20934ddef0aba38b8f1aad980cfff253/apprise/plugins/NotifyIFTTT.py#L356-L359). The problem has been patched in release version 0.9.5.1. Users who are unable to upgrade are advised to remove `apprise/plugins/NotifyIFTTT.py` to eliminate the service.	7.5	More Details
CVE-2021-3795	semver-regex is vulnerable to Inefficient Regular Expression Complexity	7.5	More Details
CVE-2021-41079	Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.	7.5	More Details
CVE-2021-29750	IBM QRadar SIEM 7.3 and 7.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 201778.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39215	Jitsi Meet is an open source video conferencing application. In versions prior to 2.0.5963, a Prosody module allows the use of symmetrical algorithms to validate JSON web tokens. This means that tokens generated by arbitrary sources can be used to gain authorization to protected rooms. This issue is fixed in Jitsi Meet 2.0.5963. There are no known workarounds aside from updating.	7.5	More Details
CVE-2021-33692	SAP Cloud Connector, version - 2.0, allows the upload of zip files as backup. This backup file can be tricked to inject special elements such as '..' and '/' separators, for attackers to escape outside of the restricted location to access files or directories.	7.5	More Details
CVE-2020-26301	ssh2 is client and server modules written in pure JavaScript for node.js. In ssh2 before version 1.4.0 there is a command injection vulnerability. The issue only exists on Windows. This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input. This is fixed in version 1.4.0.	7.5	More Details
CVE-2021-41531	NLnet Labs Routinator prior to 0.10.0 produces invalid RTR payload if an RPKI CA uses too large values in the max-length parameter in a ROA. This will lead to RTR clients such as routers to reject the RPKI data set, effectively disabling Route Origin Validation.	7.5	More Details
CVE-2021-37419	Zoho ManageEngine ADSelfService Plus before 6112 is vulnerable to SSRF.	7.5	More Details
CVE-2021-39239	A vulnerability in XML processing in Apache Jena, in versions up to 4.1.0, may allow an attacker to execute XML External Entities (XXE), including exposing the contents of local files to a remote server.	7.5	More Details
CVE-2021-36160	A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).	7.5	More Details
CVE-2021-34798	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.	7.5	More Details
CVE-2020-35340	A local file inclusion vulnerability in ExpertPDF 9.5.0 through 14.1.0 allows attackers to read the file contents from files that the running ExpertPDF process has access to read.	7.5	More Details
CVE-2021-36960	Windows SMB Information Disclosure Vulnerability	7.5	More Details
CVE-2021-31843	Improper privileges management vulnerability in McAfee Endpoint Security (ENS) Windows prior to 10.7.0 September 2021 Update allows local users to access files which they would otherwise not have access to via manipulating junction links to redirect McAfee folder operations to an unintended location.	7.3	More Details
CVE-2021-3796	vim is vulnerable to Use After Free	7.3	More Details
CVE-2021-39128	Affected versions of Atlassian Jira Server or Data Center using the Jira Service Management addon allow remote attackers with JIRA Administrators access to execute arbitrary Java code via a server-side template injection vulnerability in the Email Template feature. The affected versions of Jira Server or Data Center are before version 8.13.12, and from version 8.14.0 before 8.19.1.	7.2	More Details
CVE-2021-24403	The Orders functionality in the WordPress Page Contact plugin through 1.0 has an order_id parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. The feature is available to low privilege users such as contributors	7.2	More Details
CVE-2021-24397	The edit functionality in the MicroCopy WordPress plugin through 1.1.0 makes a get request to fetch the related option. The id parameter used is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	7.2	More Details
CVE-2021-24398	The Add new scene functionality in the Responsive 3D Slider WordPress plugin through 1.2 uses an id parameter which is not sanitised, escaped or validated before being inserted to a SQL statement, leading to SQL injection. This is a time based SQLI and in the same function vulnerable parameter is passed twice so if we pass time as 5 seconds it takes 10 seconds to return since the query is ran twice.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24399	The check_order function of The Sorter WordPress plugin through 1.0 uses an `area_id` parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	7.2	More Details
CVE-2020-21483	An arbitrary file upload vulnerability in Jizhicms v1.5 allows attackers to execute arbitrary code via a crafted .jpg file which is later changed to a PHP file.	7.2	More Details
CVE-2021-24396	A pageid GET parameter of the GSEOR – WordPress SEO Plugin WordPress plugin through 1.3 is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	7.2	More Details
CVE-2021-24663	The Simple Schools Staff Directory WordPress plugin through 1.1 does not validate uploaded logo pictures to ensure that are indeed images, allowing high privilege users such as admin to upload arbitrary file like PHP, leading to RCE	7.2	More Details
CVE-2021-24400	The Edit Role functionality in the Display Users WordPress plugin through 2.0.0 had an `id` parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	7.2	More Details
CVE-2021-39402	MaianAffiliate v.1.0 is suffers from code injection by adding a new product via the admin panel. The injected payload is reflected on the affiliate main page for all authenticated and unauthenticated visitors.	7.2	More Details
CVE-2021-24401	The Edit domain functionality in the WP Domain Redirect WordPress plugin through 1.0 has an `editid` parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	7.2	More Details
CVE-2021-41383	setup.cgi on NETGEAR R6020 1.0.0.48 devices allows an admin to execute arbitrary shell commands via shell metacharacters in the ntp_server field.	7.2	More Details
CVE-2020-14109	There is command injection in the meshd program in the routing system, resulting in command execution under administrator authority on Xiaomi router AX3600 with ROM version =< 1.1.12	7.2	More Details
CVE-2021-24402	The Orders functionality in the WP iCommerce WordPress plugin through 1.1.1 has an `order_id` parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. The feature is available to low privilege users such as contributors	7.2	More Details
CVE-2020-21480	An arbitrary file write vulnerability in RGCMS v1.06 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2020-21481	An arbitrary file upload vulnerability in RGCMS v1.06 allows attackers to execute arbitrary code via a crafted .txt file which is later changed to a PHP file.	7.2	More Details
CVE-2021-24511	The fetch_product_ajax functionality in the Product Feed on WooCommerce WordPress plugin before 3.3.1.0 uses a `product_id` POST parameter which is not properly sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	7.2	More Details
CVE-2021-38634	Microsoft Windows Update Client Elevation of Privilege Vulnerability	7.1	More Details
CVE-2021-38649	Open Management Infrastructure Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-39205	Jitsi Meet is an open source video conferencing application. Versions prior to 2.0.6173 are vulnerable to client-side cross-site scripting via injecting properties into JSON objects that were not properly escaped. There are no known incidents related to this vulnerability being exploited in the wild. This issue is fixed in Jitsi Meet version 2.0.6173. There are no known workarounds aside from upgrading.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16630	TI's BLE stack caches and reuses the LTK's property for a bonded mobile. A LTK can be an unauthenticated-and-no-MITM-protection key created by Just Works or an authenticated-and-MITM-protection key created by Passkey Entry, Numeric Comparison or OOB. Assume that a victim mobile uses secure pairing to pair with a victim BLE device based on TI chips and generate an authenticated-and-MITM-protection LTK. If a fake mobile with the victim mobile's MAC address uses Just Works and pairs with the victim device, the generated LTK still has the property of authenticated-and-MITM-protection. Therefore, the fake mobile can access attributes with the authenticated read/write permission.	6.8	More Details
CVE-2021-39213	GLPI is a free Asset and IT management software package. Starting in version 9.1 and prior to version 9.5.6, GLPI with API Rest enabled is vulnerable to API bypass with custom header injection. This issue is fixed in version 9.5.6. One may disable API Rest as a workaround.	6.8	More Details
CVE-2021-33693	SAP Cloud Connector, version - 2.0, allows an authenticated administrator to modify a configuration file to inject malicious codes that could potentially lead to OS command execution.	6.8	More Details
CVE-2021-40067	The access controls on the Mobility read-write API improperly validate user access permissions; this API is disabled by default. If the API is manually enabled, attackers with both network access to the API and valid credentials can read and write data to it; regardless of access control group membership settings. This vulnerability is fixed in Mobility v12.14.	6.8	More Details
CVE-2021-39518	An issue was discovered in libjpeg through 2020021. LineBuffer::FetchRegion() in linebuffer.cpp has a heap-based buffer overflow.	6.5	More Details
CVE-2021-39514	An issue was discovered in libjpeg through 2020021. An uncaught floating point exception in the function ACLosslessScan::ParseMCU() located in aclosslessscan.cpp. It allows an attacker to cause Denial of Service.	6.5	More Details
CVE-2021-39515	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function SampleInterleavedLSScan::ParseMCU() located in sampleinterleavedlsscan.cpp. It allows an attacker to cause Denial of Service.	6.5	More Details
CVE-2021-39516	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function HuffmanDecoder::Get() located in huffmandecoder.hpp. It allows an attacker to cause Denial of Service.	6.5	More Details
CVE-2020-20902	A CWE-125: Out-of-bounds read vulnerability exists in long_term_filter function in g729postfilter.c in FFmpeg 4.2.1 during computation of the denominator of pseudo-normalized correlation R'(0), that could result in disclosure of information.	6.5	More Details
CVE-2021-39517	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function BlockBitmapRequester::ReconstructUnsampled() located in blockbitmaprequester.cpp. It allows an attacker to cause Denial of Service.	6.5	More Details
CVE-2021-37420	Zoho ManageEngine ADSelfService Plus before 6112 is vulnerable to mail spoofing.	6.5	More Details
CVE-2021-39519	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function BlockBitmapRequester::PullQData() located in blockbitmaprequester.cpp It allows an attacker to cause Denial of Service.	6.5	More Details
CVE-2021-24585	The Timetable and Event Schedule WordPress plugin before 2.4.0 outputs the Hashed Password, Username and Email Address (along other less sensitive data) of the user related to the Even Head of the Timeslot in the response when requesting the event Timeslot data with a user with the edit_posts capability. Combined with the other Unauthorised Event Timeslot Modification issue (https://wpscan.com/reports/submissions/4699/) where an arbitrary user ID can be set, this could allow low privilege users with the edit_posts capability (such as author) to retrieve sensitive User data by iterating over the user_id	6.5	More Details
CVE-2021-39520	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function BlockBitmapRequester::PushReconstructedData() located in blockbitmaprequester.cpp. It allows an attacker to cause Denial of Service.	6.5	More Details
CVE-2021-39521	An issue was discovered in libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function bit_read_BB() located in bits.c. It allows an attacker to cause Denial of Service.	6.5	More Details
CVE-2021-39523	An issue was discovered in libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function check_POLYLINE_handles() located in decode.c. It allows an attacker to cause Denial of Service.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39535	An issue was discovered in libxsmm through v1.16.1-93. A NULL pointer dereference exists in JIT code. It allows an attacker to cause Denial of Service.	6.5	More Details
CVE-2021-29856	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 could allow an authenticated usre to cause a denial of service through the WebGUI Map Creation page. IBM X-Force ID: 205685.	6.5	More Details
CVE-2021-39532	An issue was discovered in libslax through v0.22.1. A NULL pointer dereference exists in the function slaxLexer() located in slaxlexer.c. It allows an attacker to cause Denial of Service.	6.5	More Details
CVE-2021-41380	RealVNC Viewer 6.21.406 allows remote VNC servers to cause a denial of service (application crash) via crafted RFB protocol data. NOTE: It is asserted that this issue requires social engineering a user into connecting to a fake VNC Server. The VNC Viewer application they are using will then hang, until terminated, but no memory leak occurs - the resources are freed once the hung process is terminated and the resource usage is constant during the hang. Only the process that is connected to the fake Server is affected. This is an application bug, not a security issue	6.5	More Details
CVE-2020-21597	libde265 v1.0.4 contains a heap buffer overflow in the mc_chroma function, which can be exploited via a crafted a file.	6.5	More Details
CVE-2020-21594	libde265 v1.0.4 contains a heap buffer overflow in the put_epel_hv_fallback function, which can be exploited via a crafted a file.	6.5	More Details
CVE-2021-38629	Windows Ancillary Function Driver for WinSock Information Disclosure Vulnerability	6.5	More Details
CVE-2021-34572	Enbra EWM 1.7.29 does not check for or detect replay attacks sent by wireless M-Bus Security mode 5 devices. Instead timestamps of the sensor are replaced by the time of the readout even if the data is a replay of earlier data.	6.5	More Details
CVE-2021-34571	Multiple Wireless M-Bus devices by Enbra use Hard-coded Credentials in Security mode 5 without an option to change the encryption key. An adversary can learn all information that is available in Enbra EWM.	6.5	More Details
CVE-2020-21606	libde265 v1.0.4 contains a heap buffer overflow fault in the put_epel_16_fallback function, which can be exploited via a crafted a file.	6.5	More Details
CVE-2020-21596	libde265 v1.0.4 contains a global buffer overflow in the decode_CABAC_bit function, which can be exploited via a crafted a file.	6.5	More Details
CVE-2020-21605	libde265 v1.0.4 contains a segmentation fault in the apply_sao_internal function, which can be exploited via a crafted a file.	6.5	More Details
CVE-2020-21604	libde265 v1.0.4 contains a heap buffer overflow fault in the _mm_loadl_epi64 function, which can be exploited via a crafted a file.	6.5	More Details
CVE-2020-21603	libde265 v1.0.4 contains a heap buffer overflow in the put_qpel_0_0_fallback_16 function, which can be exploited via a crafted a file.	6.5	More Details
CVE-2021-40964	A Path Traversal vulnerability exists in TinyFileManager all version up to and including 2.4.6 that allows attackers to upload a file (with Admin credentials or with the CSRF vulnerability) with the "fullpath" parameter containing path traversal strings (../ and ..\) in order to escape the server's intended working directory and write malicious files onto any directory on the computer.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39228	Tremor is an event processing system for unstructured data. A vulnerability exists between versions 0.7.2 and 0.11.6. This vulnerability is a memory safety Issue when using `patch` or `merge` on `state` and assign the result back to `state`. In this case, affected versions of Tremor and the tremor-script crate maintains references to memory that might have been freed already. And these memory regions can be accessed by retrieving the `state`, e.g. send it over TCP or HTTP. This requires the Tremor server (or any other program using tremor-script) to execute a tremor-script script that uses the mentioned language construct. The issue has been patched in version 0.11.6 by removing the optimization and always cloning the target expression of a Merge or Patch. If an upgrade is not possible, a possible workaround is to avoid the optimization by introducing a temporary variable and not immediately reassigning to `state`.	6.5	More Details
CVE-2021-20433	IBM Security Guardium 11.3 could allow a an authenticated user to obtain sensitive information that could be used in further attacks against the system. IBM X-Force ID: 196345.	6.5	More Details
CVE-2021-38624	Windows Key Storage Provider Security Feature Bypass Vulnerability	6.5	More Details
CVE-2021-41395	Teleport before 6.2.12 and 7.x before 7.1.1 allows attackers to control a database connection string, in some situations, via a crafted database name or username.	6.5	More Details
CVE-2020-21602	libde265 v1.0.4 contains a heap buffer overflow in the put_weighted_bipred_16_fallback function, which can be exploited via a crafted a file.	6.5	More Details
CVE-2021-39210	GLPI is a free Asset and IT management software package. In versions prior to 9.5.6, the cookie used to store the autologin cookie (when a user uses the "remember me" feature) is accessible by scripts. A malicious plugin that could steal this cookie would be able to use it to autologin. This issue is fixed in version 9.5.6. As a workaround, one may avoid using the "remember me" feature.	6.5	More Details
CVE-2020-21595	libde265 v1.0.4 contains a heap buffer overflow in the mc_luma function, which can be exploited via a crafted a file.	6.5	More Details
CVE-2020-21601	libde265 v1.0.4 contains a stack buffer overflow in the put_qpel_fallback function, which can be exploited via a crafted a file.	6.5	More Details
CVE-2020-19154	Improper Access Control in Jfinal CMS v4.7.1 and earlier allows remote attackers to obtain sensitive information via the 'FileManager.editFile()' function in the component 'modules/filemanager/FileManagerController.java'.	6.5	More Details
CVE-2020-19147	Improper Access Control in Jfinal CMS v4.7.1 and earlier allows remote attackers to obtain sensitive infromation via the 'getFolder()' function in the component '/modules/filemanager/FileManager.java'.	6.5	More Details
CVE-2020-19146	Improper Access Control in Jfinal CMS v4.7.1 and earlier allows remote attackers to obtain sensitive information via the 'TemplatePath' parameter in the component 'jfinal_cms/admin/folder/list'.	6.5	More Details
CVE-2021-3801	prism is vulnerable to Inefficient Regular Expression Complexity	6.5	More Details
CVE-2020-21600	libde265 v1.0.4 contains a heap buffer overflow in the put_weighted_pred_avg_16_fallback function, which can be exploited via a crafted a file.	6.5	More Details
CVE-2021-22147	Elasticsearch before 7.14.0 did not apply document and field level security to searchable snapshots. This could lead to an authenticated user gaining access to information that they are unauthorized to view.	6.5	More Details
CVE-2020-21599	libde265 v1.0.4 contains a heap buffer overflow in the de265_image::available_zscan function, which can be exploited via a crafted a file.	6.5	More Details
CVE-2021-38669	Microsoft Edge (Chromium-based) Tampering Vulnerability	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39219	Wasmtime is an open source runtime for WebAssembly & WASI. Wasmtime before version 0.30.0 is affected by a type confusion vulnerability. As a Rust library the `wasmtime` crate clearly marks which functions are safe and which are `unsafe`, guaranteeing that if consumers never use `unsafe` then it should not be possible to have memory unsafety issues in their embeddings of Wasmtime. An issue was discovered in the safe API of `Linker::func_*` APIs. These APIs were previously not sound when one `Engine` was used to create the `Linker` and then a different `Engine` was used to create a `Store` and then the `Linker` was used to instantiate a module into that `Store`. Cross-`Engine` usage of functions is not supported in Wasmtime and this can result in type confusion of function pointers, resulting in being able to safely call a function with the wrong type. Triggering this bug requires using at least two `Engine` values in an embedding and then additionally using two different values with a `Linker` (one at the creation time of the `Linker` and another when instantiating a module with the `Linker`). It's expected that usage of more-than-one `Engine` in an embedding is relatively rare since an `Engine` is intended to be a globally shared resource, so the expectation is that the impact of this issue is relatively small. The fix implemented is to change this behavior to `panic!()` in Rust instead of silently allowing it. Using different `Engine` instances with a `Linker` is a programmer bug that `wasmtime` catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.	6.3	More Details
CVE-2021-39218	Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.26.0 and before version 0.30.0 is affected by a memory unsoundness vulnerability. There was an invalid free and out-of-bounds read and write bug when running Wasm that uses `externref`s in Wasmtime. To trigger this bug, Wasmtime needs to be running Wasm that uses `externref`s, the host creates non-null `externrefs`, Wasmtime performs a garbage collection (GC), and there has to be a Wasm frame on the stack that is at a GC safepoint where there are no live references at this safepoint, and there is a safepoint with live references earlier in this frame's function. Under this scenario, Wasmtime would incorrectly use the GC stack map for the safepoint from earlier in the function instead of the empty safepoint. This would result in Wasmtime treating arbitrary stack slots as `externref`s that needed to be rooted for GC. At the *next* GC, it would be determined that nothing was referencing these bogus `externref`s (because nothing could ever reference them, because they are not really `externref`s) and then Wasmtime would deallocate them and run `<ExternRef as Drop>::drop` on them. This results in a free of memory that is not necessarily on the heap (and shouldn't be freed at this moment even if it was), as well as potential out-of-bounds reads and writes. Even though support for `externref`s (via the reference types proposal) is enabled by default, unless you are creating non-null `externref`s in your host code or explicitly triggering GCs, you cannot be affected by this bug. We have reason to believe that the effective impact of this bug is relatively small because usage of `externref` is currently quite rare. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime at this time, you can avoid this bug by disabling the reference types proposal by passing `false` to `wasmtime::Config::wasm_reference_types`.	6.3	More Details
CVE-2021-40448	Microsoft Accessibility Insights for Android Information Disclosure Vulnerability	6.3	More Details
CVE-2021-39216	Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.19.0 and before version 0.30.0 there was a use-after-free bug when passing `externref`s from the host to guest Wasm content. To trigger the bug, you have to explicitly pass multiple `externref`s from the host to a Wasm instance at the same time, either by passing multiple `externref`s as arguments from host code to a Wasm function, or returning multiple `externref`s to Wasm from a multi-value return function defined in the host. If you do not have host code that matches one of these shapes, then you are not impacted. If Wasmtime's `VMExternRefActivationsTable` became filled to capacity after passing the first `externref` in, then passing in the second `externref` could trigger a garbage collection. However the first `externref` is not rooted until we pass control to Wasm, and therefore could be reclaimed by the collector if nothing else was holding a reference to it or otherwise keeping it alive. Then, when control was passed to Wasm after the garbage collection, Wasm could use the first `externref`, which at this point has already been freed. We have reason to believe that the effective impact of this bug is relatively small because usage of `externref` is currently quite rare. The bug has been fixed, and users should upgrade to Wasmtime 0.30.0. If you cannot upgrade Wasmtime yet, you can avoid the bug by disabling reference types support in Wasmtime by passing `false` to `wasmtime::Config::wasm_reference_types`.	6.3	More Details
CVE-2021-39227	ZRender is a lightweight graphic library providing 2d draw for Apache ECharts. In versions prior to 5.2.1, using `merge` and `clone` helper methods in the `src/core/util.ts` module results in prototype pollution. It affects the popular data visualization library Apache ECharts, which uses and exports these two methods directly. The GitHub Security Advisory page for this vulnerability contains a proof of concept. This issue is patched in ZRender version 5.2.1. One workaround is available: Check if there is `__proto__` in the object keys. Omit it before using it as an parameter in these affected methods. Or in `echarts.util.merge` and `setOption` if project is using ECharts.	6.2	More Details
CVE-2021-34573	In Enbra EWM in Version 1.7.29 together with several tested wireless M-Bus Sensors the events backflow and "no flow" are not reconized or misinterpreted. This may lead to wrong values and missing events.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20829	Cross-site scripting vulnerability due to the inadequate tag sanitization in GROWI versions v4.2.19 and earlier allows remote attackers to execute an arbitrary script on the web browser of the user who accesses a specially crafted page.	6.1	More Details
CVE-2021-27340	OpenSIS Community Edition version <= 7.6 is affected by a reflected XSS vulnerability in EmailCheck.php via the "opt" parameter.	6.1	More Details
CVE-2021-20825	Cross-site scripting vulnerability in List (order management) item change plug-in (for EC-CUBE 3.0 series) Ver.1.1 and earlier allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-39325	The OptinMonster WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to insufficient input validation in the load_previews function found in the ~/OMAPI/Output.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.6.0.	6.1	More Details
CVE-2021-38657	Microsoft Office Graphics Component Information Disclosure Vulnerability	6.1	More Details
CVE-2021-20828	Cross-site scripting vulnerability in Order Status Batch Change Plug-in (for EC-CUBE 3.0 series) all versions allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-33691	NWDI Notification Service versions - 7.31, 7.40, 7.50, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.SAP NetWeaver Development Infrastructure Notification Service allows a threat actor to send crafted scripts to a victim. If the victim has an active session when the crafted script gets executed, the threat actor could compromise information in victims session, and gain access to some sensitive information also.	6.1	More Details
CVE-2020-19554	Cross Site Scripting (XSS) vulnerability exists in ManageEngine OPManager <=12.5.174 when the API key contains an XML-based XSS payload.	6.1	More Details
CVE-2021-39307	PDFTron's WebViewer UI 8.0 or below renders dangerous URLs as hyperlinks in supported documents, including JavaScript URLs, allowing the execution of arbitrary JavaScript code.	6.1	More Details
CVE-2020-19157	Cross Site Scripting (CSS) in Wenku CMS v3.4 allows remote attackers to execute arbitrary code via the 'Intro' parameter for the component '/index.php?m=ucenter&a=index'.	6.1	More Details
CVE-2021-37412	The TechRadar app 1.1 for Confluence Server allows XSS via the Title field of a Radar.	6.1	More Details
CVE-2021-40868	In Cloudron 6.2, the returnTo parameter on the login page is vulnerable to Reflected XSS.	6.1	More Details
CVE-2021-40238	A Cross Site Scriptiong (XSS) vulnerability exists in the admin panel in Webuzo < 2.9.0 via an HTTP request to a non-existent page, which is activated by administrators viewing the "Error Log" page. An attacker can leverage this to achieve Unauthenticated Remote Code Execution via the "Cron Jobs" functionality of Webuzo.	6.1	More Details
CVE-2021-33697	Under certain conditions, SAP BusinessObjects Business Intelligence Platform (SAPUI5), versions - 420, 430, can allow an unauthenticated attacker to redirect users to a malicious site due to Reverse Tabnabbing vulnerabilities.	6.1	More Details
CVE-2021-3811	adminlte is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2021-3783	yourls is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2021-3780	peertube is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19915	Cross Site Scripting (XSS vulnerability exists in WUZHI CMS 4.1.0 via the mailbox username in index.php.	6.1	More Details
CVE-2021-24657	The Limit Login Attempts WordPress plugin before 4.0.50 does not escape the IP addresses (which can be controlled by attacker via headers such as X-Forwarded-For) of attempted logins before outputting them in the reports table, leading to an Unauthenticated Stored Cross-Site Scripting issue.	6.1	More Details
CVE-2021-3812	adminlte is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2021-29795	IBM PowerVM Hypervisor FW860, FW930, FW940, and FW950 could allow a local user to create a specially crafted sequence of hypervisor calls from a partition that could crash the system. IBM X-Force ID: 203557.	6.0	More Details
CVE-2021-38632	BitLocker Security Feature Bypass Vulnerability	5.7	More Details
CVE-2021-41087	in-toto-golang is a go implementation of the in-toto framework to protect software supply chain integrity. In affected versions authenticated attackers posing as functionaries (i.e., within a trusted set of users for a layout) are able to create attestations that may bypass DISALLOW rules in the same layout. An attacker with access to trusted private keys, may issue an attestation that contains a disallowed artifact by including path traversal semantics (e.g., foo vs dir/../foo). Exploiting this vulnerability is dependent on the specific policy applied. The problem has been fixed in version 0.3.0.	5.6	More Details
CVE-2021-23444	This affects the package jointjs before 3.4.2. A type confusion vulnerability can lead to a bypass of CVE-2020-28480 when the user-provided keys used in the path parameter are arrays in the setByPath function.	5.6	More Details
CVE-2021-32276	An issue was discovered in faad2 through 2.10.0. A NULL pointer dereference exists in the function get_sample() located in output.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39549	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function file::WavFile::WavFile() located in wav_file.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39559	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function GString::~GString() located in GString.cc. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-36959	Windows Authenticode Spoofing Vulnerability	5.5	More Details
CVE-2021-39557	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function copyString() located in gmem.cc. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39556	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function InfoOutputDev::type3D1() located in InfoOutputDev.cc. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39555	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function InfoOutputDev::type3D0() located in InfoOutputDev.cc. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39554	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function Lexer::Lexer() located in Lexer.cc. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39553	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function grealloc() located in gmem.cc. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39548	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function frame::FrameDecoder::process() located in frame_decoder.c. It allows an attacker to cause Denial of Service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39547	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function lpc::SampleGenerator::process() located in sample_generator.cpp. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39545	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function rice::RiceDecoder::process() located in rice_decoder.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39543	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function Analyze::AnalyzeRoot() located in analyze.cpp. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-32275	An issue was discovered in faust through v2.30.5. A NULL pointer dereference exists in the function CosPrim::computeSigOutput() located in cosprim.hh. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39541	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function Analyze::AnalyzeXref() located in analyze.cpp. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39539	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function node::BDCNode::~BDCNode() located in bdcnode.cpp. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39538	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function node::ObjNode::Value() located in objnode.cpp. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39562	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function FileStream::makeSubStream() located in Stream.cc. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39563	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_DumpActions() located in swfaction.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-26437	Visual Studio Code Spoofing Vulnerability	5.5	More Details
CVE-2021-39575	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function dump_method() located in abc.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39598	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function callcode() located in code.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39597	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function code_dump2() located in code.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39596	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function code_parse() located in code.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39594	Other An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function updateusage() located in swftext.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39593	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_FontExtract_DefineFontInfo() located in swftext.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39592	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function pool_lookup_uint() located in pool.c. It allows an attacker to cause Denial of Service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39591	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_GetShapeBoundingBox() located in swfshape.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39590	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function params_dump() located in abc.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39589	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function parse_metadata() located in abc.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39588	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_ReadABC() located in abc.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39587	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_DumpABC() located in abc.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39585	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function traits_dump() located in abc.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39584	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function namespace_set_hash() located in pool.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-39583	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function pool_lookup_string2() located in pool.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-41061	In RIOT-OS 2021.01, nonce reuse in 802.15.4 encryption in the ieee820154_security component allows attackers to break encryption by triggering reboots.	5.5	More Details
CVE-2021-36961	Windows Installer Denial of Service Vulnerability	5.5	More Details
CVE-2021-39542	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function Font::Size() located in font.cpp. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2020-21533	fig2dev 3.2.7b contains a stack buffer overflow in the read_textobject function in read.c.	5.5	More Details
CVE-2020-21534	fig2dev 3.2.7b contains a global buffer overflow in the get_line function in read.c.	5.5	More Details
CVE-2021-38635	Windows Redirected Drive Buffering SubSystem Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2021-38636	Windows Redirected Drive Buffering SubSystem Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2021-26333	An information disclosure vulnerability exists in AMD Platform Security Processor (PSP) chipset driver. The discretionary access control list (DACL) may allow low privileged users to open a handle and send requests to the driver resulting in a potential data leak from uninitialized physical pages.	5.5	More Details
CVE-2021-36972	Windows SMB Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-21913	International Components for Unicode (ICU-20850) v66.1 was discovered to contain a use after free bug in the pkg_createWithAssemblyCode function in the file tools/pkgdata/pkgdata.cpp.	5.5	More Details
CVE-2021-36969	Windows Redirected Drive Buffering SubSystem Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2021-41525	An issue related to modification of otherwise restricted files through a locally authenticated attacker exists in FlexNet inventory agent and inventory beacon versions 2020 R2.5 and prior.	5.5	More Details
CVE-2020-21529	fig2dev 3.2.7b contains a stack buffer overflow in the bezier_spline function in genepic.c.	5.5	More Details
CVE-2020-21530	fig2dev 3.2.7b contains a segmentation fault in the read_objects function in read.c.	5.5	More Details
CVE-2020-21531	fig2dev 3.2.7b contains a global buffer overflow in the conv_pattern_index function in gencgm.c.	5.5	More Details
CVE-2021-32289	An issue was discovered in heif through through v3.6.2. A NULL pointer dereference exists in the function convertByteStreamToRBSP() located in nalutil.cpp. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2020-21532	fig2dev 3.2.7b contains a global buffer overflow in the setfigfont function in genepic.c.	5.5	More Details
CVE-2021-38637	Windows Storage Information Disclosure Vulnerability	5.5	More Details
CVE-2021-32285	An issue was discovered in gravity through 0.8.1. A NULL pointer dereference exists in the function list_iterator_next() located in gravity_core.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-32269	An issue was discovered in gpac through 20200801. A NULL pointer dereference exists in the function ilst_item_box_dump located in box_dump.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-32270	An issue was discovered in gpac through 20200801. A NULL pointer dereference exists in the function vwid_box_del located in box_code_base.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-36962	Windows Installer Information Disclosure Vulnerability	5.5	More Details
CVE-2021-32280	An issue was discovered in fig2dev before 3.2.8.. A NULL pointer dereference exists in the function compute_closed_spline() located in trans_spline.c. It allows an attacker to cause Denial of Service. The fixed version of fig2dev is 3.2.8.	5.5	More Details
CVE-2021-32282	An issue was discovered in gravity through 0.8.1. A NULL pointer dereference exists in the function ircode_add_check() located in gravity_ircode.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-32283	An issue was discovered in gravity through 0.8.1. A NULL pointer dereference exists in the function gravity_string_to_value() located in gravity_value.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2020-21535	fig2dev 3.2.7b contains a segmentation fault in the gencgm_start function in gencgm.c.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41391	In Ericsson ECM before 18.0, it was observed that Security Management Endpoint in User Profile Management Section is vulnerable to stored XSS via a name, leading to session hijacking and full account takeover.	5.4	More Details
CVE-2021-29818	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204345.	5.4	More Details
CVE-2021-29817	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204343.	5.4	More Details
CVE-2021-29809	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204270.	5.4	More Details
CVE-2021-40440	Microsoft Dynamics Business Central Cross-site Scripting Vulnerability	5.4	More Details
CVE-2020-19553	Cross Site Scripting (XSS) vlnerability exists in WUZHI CMS up to and including 4.1.0 in the config function in coreframe/app/attachment/libs/class/ckditor.class.php.	5.4	More Details
CVE-2021-29806	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204264.	5.4	More Details
CVE-2021-24525	The Shortcodes Ultimate WordPress plugin before 5.10.2 allows users with Contributor roles to perform stored XSS via shortcode attributes. Note: the plugin is inconsistent in its handling of shortcode attributes; some do escape, most don't, and there are even some attributes that are insecure by design (like [su_button]'s onclick attribute).	5.4	More Details
CVE-2021-28901	Multiple cross-site scripting (XSS) vulnerabilities exist in SITA Software Azur CMS 1.2.3.1 and earlier, which allows remote attackers to inject arbitrary web script or HTML via the (1) NOM_CLI , (2) ADRESSE , (3) ADRESSE2, (4) LOCALITE parameters to /eshop/products/json/aouCustomerAdresse; and the (5) nom_liste parameter to /eshop/products/json/addCustomerFavorite.	5.4	More Details
CVE-2021-29808	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204269.	5.4	More Details
CVE-2021-34650	The eID Easy WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the error parameter found in the ~/admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 4.6.	5.4	More Details
CVE-2021-24582	The ThinkTwit WordPress plugin before 1.7.1 did not sanitise or escape its "Consumer key" setting before outputting it its settings page, leading to a Stored Cross-Site Scripting issue.	5.4	More Details
CVE-2021-24597	The You Shang WordPress plugin through 1.0.1 does not escape its qrcode links settings, which result into Stored Cross-Site Scripting issues in frontend posts and the plugins settings page depending on the payload used	5.4	More Details
CVE-2021-24587	The Splash Header WordPress plugin before 1.20.8 doesn't sanitise and escape some of its settings while outputting them in the admin dashboard, leading to an authenticated Stored Cross-Site Scripting issue.	5.4	More Details
CVE-2020-12082	A stored cross-site scripting issue impacts certain areas of the Web UI for Code Insight v7.x releases up to and including 2020 R1 (7.11.0-64).	5.4	More Details
CVE-2021-23443	This affects the package edge.js before 5.3.2. A type confusion vulnerability can be used to bypass input sanitization when the input to be rendered is an array (instead of a string or a SafeValue), even if {{ }} are used.	5.4	More Details
CVE-2021-40966	A Stored XSS exists in TinyFileManager All version up to and including 2.4.6 in /tinyfilemanager.php when the server is given a file that contains HTML and javascript in its name. A malicious user can upload a file with a malicious filename containing javascript code and it will run on any user browser when they access the server.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29820	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204347.	5.4	More Details
CVE-2021-29821	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204348.	5.4	More Details
CVE-2021-33696	SAP BusinessObjects Business Intelligence Platform (Crystal Report), versions - 420, 430, does not sufficiently encode user controlled inputs and therefore an authorized attacker can exploit a XSS vulnerability, leading to non-permanently deface or modify displayed content from a Web site.	5.4	More Details
CVE-2021-29819	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204346.	5.4	More Details
CVE-2021-24618	The Donate With QRCode WordPress plugin before 1.4.5 does not sanitise or escape its QRCode Image setting, which result into a Stored Cross-Site Scripting (XSS). Furthermore, the plugin also does not have any CSRF and capability checks in place when saving such setting, allowing any authenticated user (as low as subscriber), or unauthenticated user via a CSRF vector to update them and perform such attack.	5.4	More Details
CVE-2021-38156	In Nagios XI before 5.8.6, XSS exists in the dashboard page (/dashboards/#) when administrative users attempt to edit a dashboard.	5.4	More Details
CVE-2021-3785	yourls is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-24635	The Visual Link Preview WordPress plugin before 2.2.3 does not enforce authorisation on several AJAX actions and has the CSRF nonce displayed for all authenticated users, allowing any authenticated user (such as subscriber) to call them and 1) Get and search through title and content of Draft post, 2) Get title of a password-protected post as well as 3) Upload an image from an URL	5.4	More Details
CVE-2020-21482	A cross-site scripting (XSS) vulnerability in RGCMS v1.06 allows attackers to obtain the administrator's cookie via a crafted payload in the Name field under the Message Board module	5.4	More Details
CVE-2020-19158	Cross Site Scripting (XSS) in S-CMS build 20191014 and earlier allows remote attackers to execute arbitrary code via the 'Site Title' parameter of the component '/data/admin/#/app/config/'.	5.4	More Details
CVE-2021-24584	The Timetable and Event Schedule WordPress plugin before 2.4.2 does not have proper access control when updating a timeslot, allowing any user with the edit_posts capability (contributor+) to update arbitrary timeslot from any events. Furthermore, no CSRF check is in place as well, allowing such attack to be perform via CSRF against a logged in with such capability. In versions before 2.3.19, the lack of sanitisation and escaping in some of the fields, like the descritption could also lead to Stored XSS issues	5.4	More Details
CVE-2020-19156	Cross Site Scripting (XSS) in Ari Adminer v1 allows remote attackers to execute arbitrary code via the 'Title' parameter of the 'Add New Connections' component when the 'save()' function is called.	5.4	More Details
CVE-2021-24637	The Google Fonts Typography WordPress plugin before 3.0.3 does not escape and sanitise some of its block settings, allowing users with as role as low as Contributor to perform Stored Cross-Site Scripting attacks via blockType (combined with content), align, color, variant and fontID argument of a Gutenberg block.	5.4	More Details
CVE-2021-24640	The WordPress Slider Block Gutenslider plugin before 5.2.0 does not escape the minWidth attribute of a Gutenburg block, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks	5.4	More Details
CVE-2020-19148	Cross Site Scripting (XSS) in Jfinal CMS v4.7.1 and earlier allows remote attackers to execute arbitrary code via the 'Nickname' parameter in the component '/jfinal_cms/front/person/profile.html'.	5.4	More Details
CVE-2021-29773	IBM Security Guardium 10.6 and 11.3 could allow a remote authenticated attacker to obtain sensitive information or modify user details caused by an insecure direct object vulnerability (IDOR). IBM X-Force ID: 202865.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29807	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204265.	5.4	More Details
CVE-2021-39211	GLPI is a free Asset and IT management software package. Starting in version 9.2 and prior to version 9.5.6, the telemetry endpoint discloses GLPI and server information. This issue is fixed in version 9.5.6. As a workaround, remove the file `ajax/telemetry.php`, which is not needed for usual functions of GLPI.	5.3	More Details
CVE-2021-29842	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0 and Liberty 17.0.0.3 through 21.0.0.9 could allow a remote user to enumerate usernames due to a difference of responses from valid and invalid login attempts. IBM X-Force ID: 205202.	5.3	More Details
CVE-2021-39327	The BulletProof Security WordPress plugin is vulnerable to sensitive information disclosure due to a file path disclosure in the publicly accessible ~/db_backup_log.txt file which grants attackers the full path of the site, in addition to the path of database backup files. This affects versions up to, and including, 5.1.	5.3	More Details
CVE-2021-41394	Teleport before 4.4.11, 5.x before 5.2.4, 6.x before 6.2.12, and 7.x before 7.1.1 allows alteration of build artifacts in some situations.	5.3	More Details
CVE-2021-39189	Pimcore is an open source data & experience management platform. In versions prior to 10.1.3, it is possible to enumerate usernames via the forgot password functionality. This issue is fixed in version 10.1.3. As a workaround, one may apply the available patch manually.	5.3	More Details
CVE-2020-21122	UReport v2.2.9 contains a Server-Side Request Forgery (SSRF) in the designer page which allows attackers to detect intranet device ports.	5.3	More Details
CVE-2019-16651	An issue was discovered on Virgin Media Super Hub 3 (based on ARRIS TG2492) devices. Because their SNMP commands have insufficient protection mechanisms, it is possible to use JavaScript and DNS rebinding to leak the WAN IP address of a user (if they are using certain VPN implementations, this would decloak them).	5.3	More Details
CVE-2016-20012	OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product	5.3	More Details
CVE-2020-14130	Some js interfaces in the Xiaomi community were exposed, causing sensitive functions to be maliciously called on Xiaomi community app Affected Version <3.0.210809	5.3	More Details
CVE-2021-40066	The access controls on the Mobility read-only API improperly validate user access permissions. Attackers with both network access to the API and valid credentials can read data from it; regardless of access control group membership settings. This vulnerability is fixed in Mobility v11.76 and Mobility v12.14.	5.3	More Details
CVE-2021-3806	A path traversal vulnerability on Pardus Software Center's "extractArchive" function could allow anyone on the same network to do a man-in-the-middle and write files on the system.	5.3	More Details
CVE-2021-29763	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 under very specific conditions, could allow a local user to keep running a procedure that could cause the system to run out of memory.and cause a denial of service. IBM X-Force ID: 202267.	5.1	More Details
CVE-2021-31842	XML Entity Expansion injection vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2021 Update allows a local user to initiate high CPU and memory consumption resulting in a Denial of Service attack through carefully editing the EPDeploy.xml file and then executing the setup process.	5.0	More Details
CVE-2021-29811	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 stores user credentials in plain clear text which can be read by an authenticated admin user. IBM X-Force ID: 204329.	4.9	More Details
CVE-2021-24530	The Alojapro Widget WordPress plugin through 1.1.15 doesn't properly sanitise its Custom CSS settings, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-24609	The WP Mapa Politico Espana WordPress plugin before 3.7.0 does not sanitise or escape some of its settings before outputting them in attributes, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24604	The Availability Calendar WordPress plugin before 1.2.2 does not sanitise or escape its Category Names before outputting them in page/post where the associated shortcode is embed, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed	4.8	More Details
CVE-2021-24600	The WP Dialog WordPress plugin through 1.2.5.5 does not sanitise and escape some of its settings before outputting them in pages, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-24596	The youForms for WordPress plugin through 1.0.5 does not sanitise escape the Button Text field of its Templates, allowing high privilege users (editors and admins) to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-24613	The Post Views Counter WordPress plugin before 1.3.5 does not sanitise or escape its Post Views Label settings, which could allow high privilege users to perform Cross-Site Scripting attacks in the frontend even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-33694	SAP Cloud Connector, version - 2.0, does not sufficiently encode user-controlled inputs, allowing an attacker with Administrator rights, to include malicious codes that get stored in the database, and when accessed, could be executed in the application, resulting in Stored Cross-Site Scripting.	4.8	More Details
CVE-2021-38899	IBM Cloud Pak for Data 2.5 could allow a local user with special privileges to obtain highly sensitive information. IBM X-Force ID: 209575.	4.4	More Details
CVE-2021-36956	Azure Sphere Information Disclosure Vulnerability	4.4	More Details
CVE-2021-29752	IBM Db2 11.2 and 11.5 contains an information disclosure vulnerability, exposing remote storage credentials to privileged users under specific conditions. IBM X-Fporce ID: 201780.	4.4	More Details
CVE-2021-39208	SharpCompress is a fully managed C# library to deal with many compression types and formats. Versions prior to 0.29.0 are vulnerable to partial path traversal. SharpCompress recreates a hierarchy of directories under destinationDirectory if ExtractFullPath is set to true in options. In order to prevent extraction outside the destination directory the destinationFileName path is verified to begin with fullDestinationDirectoryPath. However, prior to version 0.29.0, it is not enforced that fullDestinationDirectoryPath ends with slash. If the destinationDirectory is not slash terminated like `/home/user/dir` it is possible to create a file with a name thats begins as the destination directory one level up from the directory, i.e. `/home/user/dir.sh`. Because of the file name and destination directory constraints the arbitrary file creation impact is limited and depends on the use case. This issue is fixed in SharpCompress version 0.29.0.	4.3	More Details
CVE-2021-34576	In Kaden PICOFLUX Air in all known versions an information exposure through observable discrepancy exists. This may give sensitive information (water consumption without distinct values) to third parties.	4.3	More Details
CVE-2020-21321	emlog v6.0 contains a Cross-Site Request Forgery (CSRF) via /admin/link.php?action=addlink, which allows attackers to arbitrarily add articles.	4.3	More Details
CVE-2021-24583	The Timetable and Event Schedule WordPress plugin before 2.4.2 does not have proper access control when deleting a timeslot, allowing any user with the edit_posts capability (contributor+) to delete arbitrary timeslot from any events. Furthermore, no CSRF check is in place as well, allowing such attack to be performed via CSRF against a logged in with such capability	4.3	More Details
CVE-2020-8561	A security issue was discovered in Kubernetes where actors that control the responses of MutatingWebhookConfiguration or ValidatingWebhookConfiguration requests are able to redirect kube-apiserver requests to private networks of the apiserver. If that user can view kube-apiserver logs when the log level is set to 10, they can view the redirected responses and headers in the logs.	4.1	More Details
CVE-2021-25740	A security issue was discovered with Kubernetes that could enable users to send network traffic to locations they would otherwise not have access to via a confused deputy attack.	3.1	More Details
CVE-2018-20686	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35540	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-35541	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-20897	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-22035. Reason: This candidate is a duplicate of CVE-2020-22035. Notes: All CVE users should reference CVE-2020-22035 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-20893	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-22030. Reason: This candidate is a duplicate of CVE-2020-22030. Notes: All CVE users should reference CVE-2020-22030 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-20894	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-22025. Reason: This candidate is a duplicate of CVE-2020-22025. Notes: All CVE users should reference CVE-2020-22025 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-20895	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-22028. Reason: This candidate is a duplicate of CVE-2020-22028. Notes: All CVE users should reference CVE-2020-22028 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-20899	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-22036. Reason: This candidate is a duplicate of CVE-2020-22036. Notes: All CVE users should reference CVE-2020-22036 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-20900	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-22032. Reason: This candidate is a duplicate of CVE-2020-22032. Notes: All CVE users should reference CVE-2020-22032 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-20901	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-22022. Reason: This candidate is a duplicate of CVE-2020-22022. Notes: All CVE users should reference CVE-2020-22022 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-38089	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-22035. Reason: This candidate is a duplicate of CVE-2020-22035. Notes: All CVE users should reference CVE-2020-22035 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-41076	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-23441	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details