SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 01 December 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-2021-24915	The Contest Gallery WordPress plugin before 13.1.0.6 does not have capability checks and does not sanitise or escape the cg-search-user-name-original parameter before using it in a SQL statement when exporting users from a gallery, which could allow unauthenticated to perform SQL injections attacks, as well as get the list of all users registered on the blog, including their username and email address	9.8	More Details
CVE-2021-20850	PowerCMS XMLRPC API of PowerCMS 5.19 and earlier, PowerCMS 4.49 and earlier, PowerCMS 3.295 and earlier, and PowerCMS 2 Series (End-of-Life, EOL) allows a remote attacker to execute an arbitrary OS command via unspecified vectors.	9.8	More Details
CVE-2021-42099	Zoho ManageEngine M365 Manager Plus before 4421 is vulnerable to file-upload remote code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43202	In JetBrains TeamCity before 2021.1.3, the X-Frame-Options header is missing in some cases.	9.8	More Details
CVE-2021-41679	A SQL injection vulnerability exists in version 8.0 of openSIS when MySQL or MariaDB is used as the application database. An attacker can then issue the SQL command through the /opensis/modules/grades/InputFinalGrades.php, period parameter.	9.8	More Details
CVE-2021-41678	A SQL injection vulnerability exists in version 8.0 of openSIS when MySQL or MariaDB is used as the application database. An attacker can then issue the SQL command through the /opensis/modules/users/Staff.php, staff{TITLE] parameter.	9.8	More Details
CVE-2021-41677	A SQL injection vulnerability exists in version 8.0 of openSIS when MySQL or MariaDB is used as the application database. An attacker can then issue the SQL command through the /opensis/functions/GetStuListFnc.php &Grade= parameter.	9.8	More Details
CVE-2021-44427	An unauthenticated SQL Injection vulnerability in Rosario Student Information System (aka rosariosis) before 8.1.1 allows remote attackers to execute PostgreSQL statements (e.g., SELECT, INSERT, UPDATE, and DELETE) through /Side.php via the syear parameter.	9.8	More Details
CVE-2021-43786	Nodebb is an open source Node.js based forum software. In affected versions incorrect logic present in the token verification step unintentionally allowed master token access to the API. The vulnerability has been patch as of v1.18.5. Users are advised to upgrade as soon as possible.	9.8	More Details
CVE-2021-43691	tripexpress v1.1 is affected by a path manipulation vulnerability in file system/helpers/dompdf/load_font.php. The variable src is coming from $_SERVER["argv"] then there is a path manipulation vulnerability.	9.8	More Details
CVE-2021-43693	vesta 0.9.8-24 is affected by a file inclusion vulnerability in file web/add/user/index.php.	9.8	More Details
CVE-2021-43319	Zoho ManageEngine Network Configuration Manager before 125488 is vulnerable to command injection due to improper validation in the Ping functionality.	9.8	More Details
CVE-2021-44077	Zoho ManageEngine ServiceDesk Plus before 11306, ServiceDesk Plus MSP before 10530, and SupportCenter Plus before 11014 are vulnerable to unauthenticated remote code execution. This is related to /RestAPI URLs in a servlet, and ImportTechnicians in the Struts configuration.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44093	A Remote Command Execution vulnerability on the background in zrlog 2.2.2, at the upload avatar function, could bypass the original limit, upload the JSP file to get a WebShell	9.8	More Details
CVE-2021-38685	A command injection vulnerability has been reported to affect QNAP device, VioStor. If exploited, this vulnerability allows remote attackers to run arbitrary commands. We have already fixed this vulnerability in the following versions of QVR: QVR FW 5.1.6 build 20211109 and later	9.8	More Details
CVE-2021-44219	Gin-Vue-Admin before 2.4.6 mishandles a SQL database.	9.8	More Details
CVE-2021-34423	A buffer overflow vulnerability was discovered in Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows) before version 5.8.4, Zoom Client for Meetings for Blackberry (for Android and iOS) before version 5.8.1, Zoom Client for Meetings for intune (for Android and iOS) before version 5.8.4, Zoom Client for Meetings for Chrome OS before version 5.0.1, Zoom Rooms for Conference Room (for Android, AndroidBali, macOS, and Windows) before version 5.8.3, Controllers for Zoom Rooms (for Android, iOS, and Windows) before version 5.8.3, Zoom VDI Windows Meeting Client before version 5.8.4, Zoom VDI Azure Virtual Desktop Plugins (for Windows x86 or x64, IGEL x64, Ubuntu x64, HP ThinPro OS x64) before version 5.8.4.21112, Zoom VDI Citrix Plugins (for Windows x86 or x64, Mac Universal Installer & Uninstaller, IGEL x64, eLux RP6 x64, HP ThinPro OS x64, Ubuntu x64, CentOS x 64, Dell ThinOS) before version 5.8.4.21112, Zoom VDI VMware Plugins (for Windows x86 or x64, Mac Universal Installer & Uninstaller, IGEL x64, eLux RP6 x64, HP ThinPro OS x64, Ubuntu x64, CentOS x 64, Dell ThinOS) before version 5.8.4.21112, Zoom Meeting SDK for Android before version 5.7.6.1922, Zoom Meeting SDK for iOS before version 5.7.6.1082, Zoom Meeting SDK for macOS before version 5.7.6.1340, Zoom Meeting SDK for Windows before version 5.7.6.1081, Zoom Video SDK (for Android, iOS, macOS, and Windows) before version 1.1.2, Zoom On-Premise Meeting Connector Controller before version 4.8.12.20211115, Zoom On-Premise Meeting Connector MMR before version 4.8.12.20211115, Zoom On-Premise Recording Connector before version 5.1.0.65.20211116, Zoom On-Premise Virtual Room Connector before version 4.4.7266.20211117, Zoom On-Premise Virtual Room Connector Load Balancer before version 2.5.5692.20211117, Zoom Hybrid Zproxy before version 1.0.1058.20211116, and Zoom Hybrid MMR before version 4.6.20211116.131_x86-64. This can potentially allow a malicious actor to crash the service or application, or leverage this vulnerability to execute arbitrary code.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22049	The vSphere Web Client (FLEX/Flash) contains an SSRF (Server Side Request Forgery) vulnerability in the vSAN Web Client (vSAN UI) plug-in. A malicious actor with network access to port 443 on vCenter Server may exploit this issue by accessing a URL request outside of vCenter Server or accessing an internal service.	9.8	More Details
CVE-2021-41243	There is a Potential Zip Slip Vulnerability and OS Command Injection Vulnerability on the management system of baserCMS. Users with permissions to upload files may upload crafted zip files which may execute arbitrary commands on the host operating system. This is a vulnerability that needs to be addressed when the management system is used by an unspecified number of users. If you are eligible, please update to the new version as soon as possible.	9.1	More Details
CVE-2021-43778	Barcode is a GLPI plugin for printing barcodes and QR codes. GLPI instances version 2.x prior to version 2.6.1 with the barcode plugin installed are vulnerable to a path traversal vulnerability. This issue was patched in version 2.6.1. As a workaround, delete the `front/send.php` file.	9.1	More Details
CVE-2021-44140	Remote attackers may delete arbitrary files in a system hosting a JSPWiki instance, versions up to 2.11.0.M8, by using a carefuly crafted http request on logout, given that those files are reachable to the user running the JSPWiki instance. Apache JSPWiki users should upgrade to 2.11.0 or later.	9.1	More Details
CVE-2021-43787	Nodebb is an open source Node.js based forum software. In affected versions a prototype pollution vulnerability in the uploader module allowed a malicious user to inject arbitrary data (i.e. javascript) into the DOM, theoretically allowing for an account takeover when used in conjunction with a path traversal vulnerability disclosed at the same time as this report. The vulnerability has been patched as of v1.18.5. Users are advised to upgrade as soon as possible.	9.0	More Details
CVE-2021-3554	Improper Access Control vulnerability in the patchesUpdate API as implemented in Bitdefender Endpoint Security Tools for Linux as a relay role allows an attacker to manipulate the remote address used for pulling patches. This issue affects: Bitdefender Endpoint Security Tools for Linux versions prior to 6.6.27.390; versions prior to 7.1.2.33. Bitdefender Unified Endpoint versions prior to 6.2.21.160. Bitdefender GravityZone versions prior to 6.24.1-1.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2021-28704	PoD operations on misaligned GFNs T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] x86 HVM and PVH guests may be started in populate-on-demand (PoD) mode, to provide a way for them to later easily have more memory assigned. Guests are permitted to control certain P2M aspects of individual pages via hypercalls. These hypercalls may act on ranges of pages specified via page orders (resulting in a power-of-2 number of pages). The implementation of some of these hypercalls for PoD does not enforce the base page frame number to be suitably aligned for the specified order, yet some code involved in PoD handling actually makes such an assumption. These operations are XENMEM_decrease_reservation (CVE-2021-28704) and XENMEM_populate_physmap (CVE-2021-28707), the latter usable only by domains controlling the guest, i.e. a de-privileged qemu or a stub domain. (Patch 1, combining the fix to both these two issues.) In addition handling of XENMEM_decrease_reservation can also trigger a host crash when the specified page order is neither 4k nor 2M nor 1G (CVE-2021-28708, patch 2).	8.8	More Details
CVE-2021-42358	The Contact Form With Captcha WordPress plugin is vulnerable to Cross-Site Request Forgery due to missing nonce validation in the ~/cfwc-form.php file during contact form submission, which made it possible for attackers to inject arbitrary web scripts in versions up to, and including 1.6.2.	8.8	More Details
CVE-2021-20846	Cross-site request forgery (CSRF) vulnerability in Push Notifications for WordPress (Lite) versions prior to 6.0.1 allows a remote attacker to hijack the authentication of an administrator and conduct an arbitrary operation via a specially crafted web page.	8.8	More Details
CVE-2021-22957	A Cross-Origin Resource Sharing (CORS) vulnerability found in UniFi Protect application Version 1.19.2 and earlier allows a malicious actor who has convinced a privileged user to access a URL with malicious code to take over said user’s account.This vulnerability is fixed in UniFi Protect application Version 1.20.0 and later.	8.8	More Details
CVE-2021-38686	An improper authentication vulnerability has been reported to affect QNAP device, VioStor. If exploited, this vulnerability allows attackers to compromise the security of the system. We have already fixed this vulnerability in the following versions of QVR: QVR FW 5.1.6 build 20211109 and later	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43283	An issue was discovered on Victure WR1200 devices through 1.0.3. A command injection vulnerability was found within the web interface of the device, allowing an attacker with valid credentials to inject arbitrary shell commands to be executed by the device with root privileges. This occurs in the ping and traceroute features. An attacker would thus be able to use this vulnerability to open a reverse shell on the device with root privileges.	8.8	More Details
CVE-2021-36807	An authenticated user could potentially execute code via an SQLi vulnerability in the user portal of SG UTM before version 9.708 MR8.	8.8	More Details
CVE-2021-42364	The Stetic WordPress plugin is vulnerable to Cross-Site Request Forgery due to missing nonce validation via the stats_page function found in the ~/stetic.php file, which made it possible for attackers to inject arbitrary web scripts in versions up to, and including 1.0.6.	8.8	More Details
CVE-2020-7879	This issue was discovered when the ipTIME C200 IP Camera was synchronized with the ipTIME NAS. It is necessary to extract value for ipTIME IP camera because the ipTIME NAS send ans setCookie('[COOKIE]') . The value is transferred to the --header option in wget binary, and there is no validation check. This vulnerability allows remote attackers to execute remote command.	8.8	More Details
CVE-2021-20845	Cross-site request forgery (CSRF) vulnerability in Unlimited Sitemap Generator versions prior to v8.2 allows a remote attacker to hijack the authentication of an administrator and conduct arbitrary operation via a specially crafted web page.	8.8	More Details
CVE-2021-24755	The myCred WordPress plugin before 2.3 does not validate or escape the fields parameter before using it in a SQL statement, leading to an SQL injection exploitable by any authenticated user	8.8	More Details
CVE-2021-36328	Dell EMC Streaming Data Platform versions before 1.3 contain a SQL Injection Vulnerability. A remote malicious user may potentially exploit this vulnerability to execute SQL commands to perform unauthorized actions and retrieve sensitive information from the database.	8.8	More Details
CVE-2021-24748	The Email Before Download WordPress plugin before 6.8 does not properly validate and escape the order and orderby GET parameters before using them in SQL statements, leading to authenticated SQL injection issues	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8922	A heap-based buffer overflow was discovered in bluetoothd in BlueZ through 5.48. There isn't any check on whether there is enough space in the destination buffer. The function simply appends all data passed to it. The values of all attributes that are requested are appended to the output buffer. There are no size checks whatsoever, resulting in a simple heap overflow if one can craft a request where the response is large enough to overflow the preallocated buffer. This issue exists in service_attr_req gets called by process_request (in sdpd-request.c), which also allocates the response buffer.	8.8	More Details
CVE-2021-28708	PoD operations on misaligned GFNs T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] x86 HVM and PVH guests may be started in populate-on-demand (PoD) mode, to provide a way for them to later easily have more memory assigned. Guests are permitted to control certain P2M aspects of individual pages via hypercalls. These hypercalls may act on ranges of pages specified via page orders (resulting in a power-of-2 number of pages). The implementation of some of these hypercalls for PoD does not enforce the base page frame number to be suitably aligned for the specified order, yet some code involved in PoD handling actually makes such an assumption. These operations are XENMEM_decrease_reservation (CVE-2021-28704) and XENMEM_populate_physmap (CVE-2021-28707), the latter usable only by domains controlling the guest, i.e. a de-privileged qemu or a stub domain. (Patch 1, combining the fix to both these two issues.) In addition handling of XENMEM_decrease_reservation can also trigger a host crash when the specified page order is neither 4k nor 2M nor 1G (CVE-2021-28708, patch 2).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28707	PoD operations on misaligned GFNs T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] x86 HVM and PVH guests may be started in populate-on-demand (PoD) mode, to provide a way for them to later easily have more memory assigned. Guests are permitted to control certain P2M aspects of individual pages via hypercalls. These hypercalls may act on ranges of pages specified via page orders (resulting in a power-of-2 number of pages). The implementation of some of these hypercalls for PoD does not enforce the base page frame number to be suitably aligned for the specified order, yet some code involved in PoD handling actually makes such an assumption. These operations are XENMEM_decrease_reservation (CVE-2021-28704) and XENMEM_populate_physmap (CVE-2021-28707), the latter usable only by domains controlling the guest, i.e. a de-privileged qemu or a stub domain. (Patch 1, combining the fix to both these two issues.) In addition handling of XENMEM_decrease_reservation can also trigger a host crash when the specified page order is neither 4k nor 2M nor 1G (CVE-2021-28708, patch 2).	8.8	More Details
CVE-2021-28706	guests may exceed their designated memory limit When a guest is permitted to have close to 16TiB of memory, it may be able to issue hypercalls to increase its memory allocation beyond the administrator established limit. This is a result of a calculation done with 32-bit precision, which may overflow. It would then only be the overflowed (and hence small) number which gets compared against the established upper bound.	8.6	More Details
CVE-2021-36916	The SQL injection vulnerability in the Hide My WP WordPress plugin (versions <= 6.2.3) is possible because of how the IP address is retrieved and used inside a SQL query. The function "hmwp_get_user_ip" tries to retrieve the IP address from multiple headers, including IP address headers that the user can spoof, such as "X-Forwarded-For." As a result, the malicious payload supplied in one of these IP address headers will be directly inserted into the SQL query, making SQL injection possible.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43783	@backstage/plugin-scaffolder-backend is the backend for the default Backstage software templates. In affected versions a malicious actor with write access to a registered scaffolder template is able to manipulate the template in a way that writes files to arbitrary paths on the scaffolder-backend host instance. This vulnerability can in some situation also be exploited through user input when executing a template, meaning you do not need write access to the templates. This method will not allow the attacker to control the contents of the injected file however, unless the template is also crafted in a specific way that gives control of the file contents. This vulnerability is fixed in version `0.15.14` of the `@backstage/plugin-scaffolder-backend`. This attack is mitigated by restricting access and requiring reviews when registering or modifying scaffolder templates.	8.5	More Details
CVE-2021-43790	Lucet is a native WebAssembly compiler and runtime. There is a bug in the main branch of `lucet-runtime` affecting all versions published to crates.io that allows a use-after-free in an Instance object that could result in memory corruption, data race, or other related issues. This bug was introduced early in the development of Lucet and is present in all releases. As a result of this bug, and dependent on the memory backing for the Instance objects, it is possible to trigger a use-after-free when the Instance is dropped. Users should upgrade to the main branch of the Lucet repository. Lucet no longer provides versioned releases on crates.io. There is no way to remediate this vulnerability without upgrading.	8.5	More Details
CVE-2021-42545	An insufficient session expiration vulnerability exists in Business-DNA Solutions GmbH's TopEase® Platform Version <= 7.1.27, which allows a remote attacker to reuse, spoof, or steal other user and admin sessions.	8.1	More Details
CVE-2021-36330	Dell EMC Streaming Data Platform versions before 1.3 contain an Insufficient Session Expiration Vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability to reuse old session artifacts to impersonate a legitimate user.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42306	An information disclosure vulnerability manifests when a user or an application uploads unprotected private key data as part of an authentication certificate keyCredential on an Azure AD Application or Service Principal (which is not recommended). This vulnerability allows a user or service in the tenant with application read access to read the private key data that was added to the application. Azure AD addressed this vulnerability by preventing disclosure of any private key values added to the application. Microsoft has identified services that could manifest this vulnerability, and steps that customers should take to be protected. Refer to the FAQ section for more information. For more details on this issue, please refer to the MSRC Blog Entry.	8.1	More Details
CVE-2021-26611	HejHome GKW-IC052 IP Camera contained a hard-coded credentials vulnerability. This issue allows remote attackers to operate the IP Camera.(reboot, factory reset, snapshot etc..)	8.1	More Details
CVE-2021-42118	Persistent Cross Site Scripting in Web Applications operating on Business-DNA Solutions GmbH’s TopEase® Platform Version <= 7.1.27 via the Structure Component allows an authenticated remote attacker with Object Modification privileges to inject arbitrary HTML and JavaScript code in an object attribute, which is then rendered in the Structure Component, to alter the intended functionality and steal cookies, the latter allowing for account takeover.	8.1	More Details
CVE-2021-41192	Redash is a package for data visualization and sharing. If an admin sets up Redash versions 10.0.0 and prior without explicitly specifying the `REDASH_COOKIE_SECRET` or `REDASH_SECRET_KEY` environment variables, a default value is used for both that is the same across all installations. In such cases, the instance is vulnerable to attackers being able to forge sessions using the known default value. This issue only affects installations where the `REDASH_COOKIE_SECRET or REDASH_SECRET_KEY` environment variables have not been explicitly set. This issue does not affect users of the official Redash cloud images, Redash's Digital Ocean marketplace droplets, or the scripts in the `getredash/setup` repository. These instances automatically generate unique secret keys during installation. One can verify whether one's instance is affected by checking the value of the `REDASH_COOKIE_SECRET` environment variable. If it is `c292a0a3aa32397cdb050e233733900f`, should follow the steps to secure the instance, outlined in the GitHub Security Advisory.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42115	Missing HTTPOnly flag in Web Applications operating on Business-DNA Solutions GmbH's TopEase® Platform Version <= 7.1.27 allows an unauthenticated remote attacker to escalate privileges from unauthenticated to authenticated user via stealing and injecting the session- independent and static cookie UID.	8.1	More Details
CVE-2021-44223	WordPress before 5.8 lacks support for the Update URI plugin header. This makes it easier for remote attackers to execute arbitrary code via a supply-chain attack against WordPress installations that use any plugin for which the slug satisfies the naming constraints of the WordPress.org Plugin Directory but is not yet present in that directory.	8.1	More Details
CVE-2021-26612	An improper input validation leading to arbitrary file creation was discovered in copy method of Nexacro platform. Remote attackers use copy method to execute arbitrary command after the file creation included malicious code.	8.1	More Details
CVE-2021-38873	IBM Planning Analytics 2.0 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 208396.	7.8	More Details
CVE-2021-43771	Trend Micro Antivirus for Mac 2021 v11 (Consumer) is vulnerable to an improper access control privilege escalation vulnerability that could allow an attacker to establish a connection that could lead to full local privilege escalation within the application. Please note that an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2021-26615	ARK library allows attackers to execute remote code via the parameter(path value) of Ark_NormalizeAndDupPAthNameW function because of an integer overflow.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28705	issues with partially successful P2M updates on x86 T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] x86 HVM and PVH guests may be started in populate-on-demand (PoD) mode, to provide a way for them to later easily have more memory assigned. Guests are permitted to control certain P2M aspects of individual pages via hypercalls. These hypercalls may act on ranges of pages specified via page orders (resulting in a power-of-2 number of pages). In some cases the hypervisor carries out the requests by splitting them into smaller chunks. Error handling in certain PoD cases has been insufficient in that in particular partial success of some operations was not properly accounted for. There are two code paths affected - page removal (CVE-2021-28705) and insertion of new pages (CVE-2021-28709). (We provide one patch which combines the fix to both issues.)	7.8	More Details
CVE-2021-44198	DLL hijacking could lead to local privilege escalation. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035	7.8	More Details
CVE-2021-43284	An issue was discovered on Victure WR1200 devices through 1.0.3. The root SSH password never gets updated from its default value of admin. This enables an attacker to gain control of the device through SSH (regardless of whether the admin password was changed on the web interface).	7.8	More Details
CVE-2021-44094	ZrLog 2.2.2 has a remote command execution vulnerability at plugin download function, it could execute any JAR file	7.8	More Details
CVE-2021-31822	When Octopus Tentacle is installed on a Linux operating system, the systemd service file permissions are misconfigured. This could lead to a local unprivileged user modifying the contents of the systemd service file to gain privileged access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28709	issues with partially successful P2M updates on x86 T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] x86 HVM and PVH guests may be started in populate-on-demand (PoD) mode, to provide a way for them to later easily have more memory assigned. Guests are permitted to control certain P2M aspects of individual pages via hypercalls. These hypercalls may act on ranges of pages specified via page orders (resulting in a power-of-2 number of pages). In some cases the hypervisor carries out the requests by splitting them into smaller chunks. Error handling in certain PoD cases has been insufficient in that in particular partial success of some operations was not properly accounted for. There are two code paths affected - page removal (CVE-2021-28705) and insertion of new pages (CVE-2021-28709). (We provide one patch which combines the fix to both issues.)	7.8	More Details
CVE-2021-41279	BaserCMS is an open source content management system with a focus on Japanese language support. In affected versions users with upload privilege may upload crafted zip files capable of path traversal on the host operating system. This is a vulnerability that needs to be addressed when the management system is used by an unspecified number of users. If you are eligible, please update to the new version as soon as possible.	7.7	More Details
CVE-2021-43785	@joeattardi/emoji-button is a Vanilla JavaScript emoji picker component. In affected versions there are two vectors for XSS attacks: a URL for a custom emoji, and an i18n string. In both of these cases, a value can be crafted such that it can insert a `script` tag into the page and execute malicious code.	7.6	More Details
CVE-2021-34800	Sensitive information could be logged. The following products are affected: Acronis Agent (Windows, Linux, macOS) before build 27147	7.5	More Details
CVE-2020-7881	The vulnerability function is enabled when the streamer service related to the AfreecaTV communicated through web socket using 21201 port. A stack-based buffer overflow leading to remote code execution was discovered in strcpy() operate by "FanTicket" field. It is because of stored data without validation of length.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35533	Improper Input Validation vulnerability in the APDU parser in the Bidirectional Communication Interface (BCI) IEC 60870-5-104 function of Hitachi Energy RTU500 series allows an attacker to cause the receiving RTU500 CMU of which the BCI is enabled to reboot when receiving a specially crafted message. By default, BCI IEC 60870-5-104 function is disabled (not configured). This issue affects: Hitachi Energy RTU500 series CMU Firmware version 12.0.* (all versions); CMU Firmware version 12.2.* (all versions); CMU Firmware version 12.4.* (all versions).	7.5	More Details
CVE-2021-43296	Zoho ManageEngine SupportCenter Plus before 11016 is vulnerable to an SSRF attack in ActionExecutor.	7.5	More Details
CVE-2021-44428	Pinkie 2.15 allows remote attackers to cause a denial of service (daemon crash) via a TFTP read (RRQ) request, aka opcode 1.	7.5	More Details
CVE-2021-20835	Improper authorization in handler for custom URL scheme vulnerability in Android App 'Mercari (Merpay) - Marketplace and Mobile Payments App' (Japan version) versions prior to 4.49.1 allows a remote attacker to lead a user to access an arbitrary website and the website launches an arbitrary Activity of the app via the vulnerable App, which may result in Mercari account's access token being obtained.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34424	A vulnerability was discovered in the Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows) before version 5.8.4, Zoom Client for Meetings for Blackberry (for Android and iOS) before version 5.8.1, Zoom Client for Meetings for intune (for Android and iOS) before version 5.8.4, Zoom Client for Meetings for Chrome OS before version 5.0.1, Zoom Rooms for Conference Room (for Android, AndroidBali, macOS, and Windows) before version 5.8.3, Controllers for Zoom Rooms (for Android, iOS, and Windows) before version 5.8.3, Zoom VDI Windows Meeting Client before version 5.8.4, Zoom VDI Azure Virtual Desktop Plugins (for Windows x86 or x64, IGEL x64, Ubuntu x64, HP ThinPro OS x64) before version 5.8.4.21112, Zoom VDI Citrix Plugins (for Windows x86 or x64, Mac Universal Installer & Uninstaller, IGEL x64, eLux RP6 x64, HP ThinPro OS x64, Ubuntu x64, CentOS x 64, Dell ThinOS) before version 5.8.4.21112, Zoom VDI VMware Plugins (for Windows x86 or x64, Mac Universal Installer & Uninstaller, IGEL x64, eLux RP6 x64, HP ThinPro OS x64, Ubuntu x64, CentOS x 64, Dell ThinOS) before version 5.8.4.21112, Zoom Meeting SDK for Android before version 5.7.6.1922, Zoom Meeting SDK for iOS before version 5.7.6.1082, Zoom Meeting SDK for macOS before version 5.7.6.1340, Zoom Meeting SDK for Windows before version 5.7.6.1081, Zoom Video SDK (for Android, iOS, macOS, and Windows) before version 1.1.2, Zoom on-premise Meeting Connector before version 4.8.12.20211115, Zoom on-premise Meeting Connector MMR before version 4.8.12.20211115, Zoom on-premise Recording Connector before version 5.1.0.65.20211116, Zoom on-premise Virtual Room Connector before version 4.4.7266.20211117, Zoom on-premise Virtual Room Connector Load Balancer before version 2.5.5692.20211117, Zoom Hybrid Zproxy before version 1.0.1058.20211116, and Zoom Hybrid MMR before version 4.6.20211116.131_x86-64 which potentially allowed for the exposure of the state of process memory. This issue could be used to potentially gain insight into arbitrary areas of the product's memory.	7.5	More Details
CVE-2020-7880	The vulnerabilty was discovered in ActiveX module related to NeoRS remote support program. This issue allows an remote attacker to download and execute remote file. It is because of improper parameter validation of StartNeoRS function in ActiveX.	7.5	More Details
CVE-2021-42544	Missing Rate Limiting in Web Applications operating on Business-DNA Solutions GmbH’s TopEase® Platform Version <= 7.1.27 on the Login Form allows an unauthenticated remote attacker to perform multiple login attempts, which facilitates gaining privileges.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3769	# Vulnerability in `pygmalion`, `pygmalion-virtualenv` and `refined` themes **Description**: these themes use `print -P` on user-supplied strings to print them to the terminal. All of them do that on git information, particularly the branch name, so if the branch has a specially-crafted name the vulnerability can be exploited. **Fixed in**: [b3ba9978] (https://github.com/ohmyzsh/ohmyzsh/commit/b3ba9978). **Impacted areas**: - `pygmalion` theme. - `pygmalion-virtualenv` theme. - `refined` theme.	7.5	More Details
CVE-2021-44429	Serva 4.4.0 allows remote attackers to cause a denial of service (daemon crash) via a TFTP read (RRQ) request, aka opcode 1, a related issue to CVE-2013-0145.	7.5	More Details
CVE-2021-21980	The vSphere Web Client (FLEX/Flash) contains an unauthorized arbitrary file read vulnerability. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information.	7.5	More Details
CVE-2021-38283	Wipro Holmes Orchestrator 20.4.1 (20.4.1_02_11_2020) allows remote attackers to read application log files containing sensitive information via a predictable /log URI.	7.5	More Details
CVE-2021-3727	# Vulnerability in `rand-quote` and `hitokoto` plugins **Description**: the `rand-quote` and `hitokoto` fetch quotes from quotationspage.com and hitokoto.cn respectively, do some process on them and then use `print -P` to print them. If these quotes contained the proper symbols, they could trigger command injection. Given that they're an external API, it's not possible to know if the quotes are safe to use. **Fixed in**: [72928432] (https://github.com/ohmyzsh/ohmyzsh/commit/72928432). **Impacted areas**: - `rand-quote` plugin (`quote` function). - `hitokoto` plugin (`hitokoto` function).	7.5	More Details
CVE-2021-3726	# Vulnerability in `title` function **Description**: the `title` function defined in `lib/termsupport.zsh` uses `print` to set the terminal title to a user-supplied string. In Oh My Zsh, this function is always used securely, but custom user code could use the `title` function in a way that is unsafe. **Fixed in**: [a263cdac] (https://github.com/ohmyzsh/ohmyzsh/commit/a263cdac). **Impacted areas**: - `title` function in `lib/termsupport.zsh`. - Custom user code using the `title` function.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3725	Vulnerability in dirhistory plugin Description: the widgets that go back and forward in the directory history, triggered by pressing Alt-Left and Alt-Right, use functions that unsafely execute eval on directory names. If you cd into a directory with a carefully-crafted name, then press Alt-Left, the system is subject to command injection. Impacted areas: - Functions pop_past and pop_future in dirhistory plugin.	7.5	More Details
CVE-2021-38147	Wipro Holmes Orchestrator 20.4.1 (20.4.1_02_11_2020) allows remote attackers to download arbitrary files, such as reports containing sensitive information, because authentication is not required for API access to processexecution/DownloadExcelFile/Domain_Credential_Report_Excel, processexecution/DownloadExcelFile/User_Report_Excel, processexecution/DownloadExcelFile/Process_Report_Excel, processexecution/DownloadExcelFile/Infrastructure_Report_Excel, or processexecution/DownloadExcelFile/Resolver_Report_Excel.	7.5	More Details
CVE-2021-43776	Backstage is an open platform for building developer portals. In affected versions the auth-backend plugin allows a malicious actor to trick another user into visiting a vulnerable URL that executes an XSS attack. This attack can potentially allow the attacker to exfiltrate access tokens or other secrets from the user's browser. The default CSP does prevent this attack, but it is expected that some deployments have these policies disabled due to incompatibilities. This is vulnerability is patched in version `0.4.9` of `@backstage/plugin-auth-backend`.	7.4	More Details
CVE-2021-42119	Persistent Cross Site Scripting in Web Applications operating on Business-DNA Solutions GmbH’s TopEase® Platform Version <= 7.1.27 via the Search Functionality allows authenticated users with Object Modification privileges to inject arbitrary HTML and JavaScript in object attributes, which is then rendered in the Search Functionality, to alter the intended functionality and steal cookies, the latter allowing for account takeover.	7.3	More Details
CVE-2021-42123	Unrestricted File Upload in Web Applications operating on Business-DNA Solutions GmbH’s TopEase® Platform Version <= 7.1.27 in the File Upload Functions allows an authenticated remote attacker with Upload privileges to upload files with any file type, enabling client-side attacks.	7.3	More Details
CVE-2021-24889	The Ninja Forms Contact Form WordPress plugin before 3.6.4 does not escape keys of the fields POST parameter, which could allow high privilege users to perform SQL injections attacks	7.2	More Details
CVE-2021-40101	An issue was discovered in Concrete CMS before 8.5.7. The Dashboard allows a user's password to be changed without a prompt for the current password.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24860	The BSK PDF Manager WordPress plugin before 3.1.2 does not validate and escape the orderby and order parameters before using them in a SQL statement, leading to a SQL injection issue	7.2	More Details
CVE-2021-43780	Redash is a package for data visualization and sharing. In versions 10.0 and priorm the implementation of URL-loading data sources like JSON, CSV, or Excel is vulnerable to advanced methods of Server Side Request Forgery (SSRF). These vulnerabilities are only exploitable on installations where a URL-loading data source is enabled. As of time of publication, the `master` and `release/10.x.x` branches address this by applying the Advocate library for making http requests instead of the requests library directly. Users should upgrade to version 10.0.1 to receive this patch. There are a few workarounds for mitigating the vulnerability without upgrading. One can disable the vulnerable data sources entirely, by adding the following env variable to one's configuration, making them unavailable inside the webapp. One can switch any data source of certain types (viewable in the GitHub Security Advisory) to be `View Only` for all groups on the Settings > Groups > Data Sources screen. For users unable to update an admin may modify Redash's configuration through environment variables to mitigate this issue. Depending on the version of Redash, an admin may also need to run a CLI command to re-encrypt some fields in the database. The `master` and `release/10.x.x` branches as of time of publication have removed the default value for `REDASH_COOKIE_SECRET`. All future releases will also require this to be set explicitly. For existing installations, one will need to ensure that explicit values are set for the `REDASH_COOKIE_SECRET` and `REDASH_SECRET_KEY `variables.	6.8	More Details
CVE-2021-43777	Redash is a package for data visualization and sharing. In Redash version 10.0 and prior, the implementation of Google Login (via OAuth) incorrectly uses the `state` parameter to pass the next URL to redirect the user to after login. The `state` parameter should be used for a Cross-Site Request Forgery (CSRF) token, not a static and easily predicted value. This vulnerability does not affect users who do not use Google Login for their instance of Redash. A patch in the `master` and `release/10.x.x` branches addresses this by replacing `Flask-Oauthlib` with `Authlib` which automatically provides and validates a CSRF token for the state variable. The new implementation stores the next URL on the user session object. As a workaround, one may disable Google Login to mitigate the vulnerability.	6.8	More Details
CVE-2021-38967	IBM MQ Appliance 9.2 CD and 9.2 LTS could allow a local privileged user to inject and execute malicious code. IBM X-Force ID: 212441.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36917	WordPress Hide My WP plugin (versions <= 6.2.3) can be deactivated by any unauthenticated user. It is possible to retrieve a reset token which can then be used to deactivate the plugin.	6.5	More Details
CVE-2021-20841	Improper access control in Management screen of EC-CUBE 2 series 2.11.2 to 2.17.1 allows a remote authenticated attacker to bypass access restriction and to alter System settings via unspecified vectors.	6.5	More Details
CVE-2021-41270	Symfony/Serializer handles serializing and deserializing data structures for Symfony, a PHP framework for web and console applications and a set of reusable PHP components. Symfony versions 4.1.0 before 4.4.35 and versions 5.0.0 before 5.3.12 are vulnerable to CSV injection, also known as formula injection. In Symfony 4.1, maintainers added the opt-in `csv_escape_formulas` option in the `CsvEncoder`, to prefix all cells starting with `=`, `+`, `-` or `@` with a tab `\t`. Since then, OWASP added 2 chars in that list: Tab (0x09) and Carriage return (0x0D). This makes the previous prefix char (Tab `\t`) part of the vulnerable characters, and OWASP suggests using the single quote `'` for prefixing the value. Starting with versions 4.4.34 and 5.3.12, Symfony now follows the OWASP recommendations and uses the single quote `'` to prefix formulas and add the prefix to cells starting by `\t`, `\r` as well as `=`, `+`, `-` and `@`.	6.5	More Details
CVE-2021-41268	Symfony/SecurityBundle is the security system for Symfony, a PHP framework for web and console applications and a set of reusable PHP components. Since the rework of the Remember me cookie in version 5.3.0, the cookie is not invalidated when the user changes their password. Attackers can therefore maintain their access to the account even if the password is changed as long as they have had the chance to login once and get a valid remember me cookie. Starting with version 5.3.12, Symfony makes the password part of the signature by default. In that way, when the password changes, then the cookie is not valid anymore.	6.5	More Details
CVE-2021-41267	Symfony/Http-Kernel is the HTTP kernel component for Symfony, a PHP framework for web and console applications and a set of reusable PHP components. Headers that are not part of the "trusted_headers" allowed list are ignored and protect users from "Cache poisoning" attacks. In Symfony 5.2, maintainers added support for the `X-Forwarded-Prefix` headers, but this header was accessible in SubRequest, even if it was not part of the "trusted_headers" allowed list. An attacker could leverage this opportunity to forge requests containing a `X-Forwarded-Prefix` header, leading to a web cache poisoning issue. Versions 5.3.12 and later have a patch to ensure that the `X-Forwarded-Prefix` header is not forwarded to subrequests when it is not trusted.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39995	Some Huawei products use the OpenHpi software for hardware management. A function that parses data returned by OpenHpi contains an out-of-bounds read vulnerability that could lead to a denial of service. Affected product versions include: eCNS280_TD V100R005C10; eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300.	6.5	More Details
CVE-2021-43268	An issue was discovered in VxWorks 6.9 through 7. In the IKE component, a specifically crafted packet may lead to reading beyond the end of a buffer, or a double free.	6.5	More Details
CVE-2021-42120	Insufficient Input Validation in Web Applications operating on Business-DNA Solutions GmbH's TopEase® Platform Version <= 7.1.27 on all object attributes allows an authenticated remote attacker with Object Modification privileges to insert arbitrarily long strings, eventually leading to exhaustion of the underlying resource.	6.5	More Details
CVE-2021-32037	An authorized user may trigger an invariant which may result in denial of service or server exit if a relevant aggregation request is sent to a shard. Usually, the requests are sent via mongos and special privileges are required in order to know the address of the shards and to log in to the shards of an auth enabled environment. This issue affects MongoDB Server v5.0 versions prior to and including 5.0.2.	6.5	More Details
CVE-2021-43998	HashiCorp Vault and Vault Enterprise 0.11.0 up to 1.7.5 and 1.8.4 templated ACL policies would always match the first-created entity alias if multiple entity aliases exist for a specified entity and mount combination, potentially resulting in incorrect policy enforcement. Fixed in Vault and Vault Enterprise 1.7.6, 1.8.5, and 1.9.0.	6.5	More Details
CVE-2021-20842	Cross-site request forgery (CSRF) vulnerability in EC-CUBE 2 series 2.11.0 to 2.17.1 allows a remote attacker to hijack the authentication of Administrator and delete Administrator via a specially crafted web page.	6.5	More Details
CVE-2021-22095	In Spring AMQP versions 2.2.0 - 2.2.19 and 2.3.0 - 2.3.11, the Spring AMQP Message object, in its toString() method, will create a new String object from the message body, regardless of its size. This can cause an OOM Error with a large message	6.5	More Details
CVE-2021-43282	An issue was discovered on Victure WR1200 devices through 1.0.3. The default Wi-Fi WPA2 key is advertised to anyone within Wi-Fi range through the router's MAC address. The device default Wi-Fi password corresponds to the last 4 bytes of the MAC address of its 2.4 GHz network interface controller (NIC). An attacker within scanning range of the Wi-Fi network can thus scan for Wi-Fi networks to obtain the default key.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44230	PortSwigger Burp Suite Enterprise Edition before 2021.11 on Windows has weak file permissions for the embedded H2 database, which might lead to privilege escalation. This issue can be exploited by an adversary who has already compromised a valid Windows account on the server via separate means. In this scenario, the compromised account may have inherited read access to sensitive configuration, database, and log files.	6.5	More Details
CVE-2021-31787	The Bluetooth Classic implementation on Actions ATS2815 chipsets does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service and shutdown of a device by flooding the target device with LMP_features_res packets.	6.5	More Details
CVE-2021-36326	Dell EMC Streaming Data Platform, versions prior to 1.3 contain an SSL Strip Vulnerability in the User Interface (UI). A remote unauthenticated attacker could potentially exploit this vulnerability, leading to a downgrade in the communications between the client and server into an unencrypted format.	6.5	More Details
CVE-2021-36329	Dell EMC Streaming Data Platform versions before 1.3 contain an Indirect Object Reference Vulnerability. A remote malicious user may potentially exploit this vulnerability to gain sensitive information.	6.5	More Details
CVE-2019-8921	An issue was discovered in bluetoothd in BlueZ through 5.48. The vulnerability lies in the handling of a SVC_ATTR_REQ by the SDP implementation. By crafting a malicious CSTATE, it is possible to trick the server into returning more bytes than the buffer actually holds, resulting in leaking arbitrary heap data. The root cause can be found in the function service_attr_req of sdpd-request.c. The server does not check whether the CSTATE data is the same in consecutive requests, and instead simply trusts that it is the same.	6.5	More Details
CVE-2021-36919	Multiple Authenticated Reflected Cross-Site Scripting (XSS) vulnerabilities in WordPress Awesome Support plugin (versions <= 6.0.6), vulnerable parameters (&id, &assignee).	6.1	More Details
CVE-2021-20840	Cross-site scripting vulnerability in Booking Package - Appointment Booking Calendar System versions prior to 1.5.11 allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-20848	Cross-site scripting vulnerability in rwtxt versions prior to v1.8.6 allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40369	A carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the Denounce plugin, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. Apache JSPWiki users should upgrade to 2.11.0 or later.	6.1	More Details
CVE-2021-43294	Zoho ManageEngine SupportCenter Plus before 11016 is vulnerable to Reflected XSS in the Products module.	6.1	More Details
CVE-2021-43295	Zoho ManageEngine SupportCenter Plus before 11016 is vulnerable to Reflected XSS in the Accounts module.	6.1	More Details
CVE-2021-44201	Cross-site scripting (XSS) was possible in notification pop-ups. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035	6.1	More Details
CVE-2017-20008	The myCred WordPress plugin before 1.7.8 does not sanitise and escape the user parameter before outputting it back in the Points Log admin dashboard, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-43695	issabelPBX version 2.11 is affected by a Cross Site Scripting (XSS) vulnerability. In file page.backup_restore.php, the exit function will terminate the script and print the message to the user. The message will contain $_REQUEST without sanitization, then there is a XSS vulnerability.	6.1	More Details
CVE-2021-24876	The Registrations for the Events Calendar WordPress plugin before 2.7.5 does not escape the v parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-24908	The Check & Log Email WordPress plugin before 1.0.4 does not escape the d parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-43698	phpWhois (last update Jun 30 2021) is affected by a Cross Site Scripting (XSS) vulnerability. In file example.php, the exit function will terminate the script and print the message to the user. The message will contain $_GET['query'] then there is a XSS vulnerability.	6.1	More Details
CVE-2021-43696	twmap v2.91_v4.33 is affected by a Cross Site Scripting (XSS) vulnerability. In file list.php, the exit function will terminate the script and print the message to the user. The message will contain $_REQUEST then there is a XSS vulnerability.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43692	youtube-php-mirroring (last update Jun 9, 2017) is affected by a Cross Site Scripting (XSS) vulnerability in file ytproxy/index.php.	6.1	More Details
CVE-2021-43697	Workerman-ThinkPHP-Redis (last update Mar 16, 2018) is affected by a Cross Site Scripting (XSS) vulnerability. In file Controller.class.php, the exit function will terminate the script and print the message to the user. The message will contain $_GET{C('VAR_JSONP_HANDLER')] then there is a XSS vulnerability.	6.1	More Details
CVE-2021-41256	nextcloud news-android is an Android client for the Nextcloud news/feed reader app. In affected versions the Nextcloud News for Android app has a security issue by which a malicious application installed on the same device can send it an arbitrary Intent that gets reflected back, unintentionally giving read and write access to non-exported Content Providers in Nextcloud News for Android. Users should upgrade to version 0.9.9.63 or higher as soon as possible.	5.8	More Details
CVE-2021-20844	Improper neutralization of HTTP request headers for scripting syntax vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to obtain sensitive information via a specially crafted web page.	5.7	More Details
CVE-2021-23654	This affects all versions of package html-to-csv. When there is a formula embedded in a HTML page, it gets accepted without any validation and the same would be pushed while converting it into a CSV file. Through this a malicious actor can embed or generate a malicious link or execute commands via CSV files.	5.6	More Details
CVE-2021-43211	Windows 10 Update Assistant Elevation of Privilege Vulnerability	5.5	More Details
CVE-2021-39000	IBM MQ Appliance 9.2 CD and 9.2 LTS could allow a local attacker to obtain sensitive information by inclusion of sensitive data within diagnostics. IBM X-Force ID: 213215.	5.5	More Details
CVE-2021-38999	IBM MQ Appliance could allow a local attacker to obtain sensitive information by inclusion of sensitive data within trace.	5.5	More Details
CVE-2021-38958	IBM MQ Appliance 9.2 CD and 9.2 LTS is affected by a denial of service attack caused by a concurrency issue. IBM X-Force ID: 212042	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44199	DLL hijacking could lead to denial of service. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27305, Acronis Cyber Protect Home Office (Windows) before build 39612	5.5	More Details
CVE-2021-40833	A vulnerability affecting F-Secure antivirus engine was discovered whereby unpacking UPX file can lead to denial-of-service. The vulnerability can be exploited remotely by an attacker. A successful attack will result in denial-of-service of the antivirus engine.	5.5	More Details
CVE-2021-24745	The About Author Box WordPress plugin before 1.0.2 does not sanitise and escape the Social Profiles field values before outputting them in attributes, which could allow user with a role as low as contributor to perform Cross-Site Scripting attacks.	5.4	More Details
CVE-2021-44200	Self cross-site scripting (XSS) was possible on devices page. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035	5.4	More Details
CVE-2021-24751	The GenerateBlocks WordPress plugin before 1.4.0 does not validate the generateblocks/container block's tagName attribute, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks.	5.4	More Details
CVE-2021-42564	An open redirect through HTML injection in confidential messages in Cryptshare before 5.1.0 allows remote attackers (with permission to provide confidential messages via Cryptshare) to redirect targeted victims to any URL via the '<meta http-equiv="refresh"' substring in the editor parameter.	5.4	More Details
CVE-2021-24822	The Stylish Cost Calculator WordPress plugin before 7.0.4 does not have any authorisation and CSRF checks on some of its AJAX actions (available to authenticated users), which could allow any authenticated users, such as subscriber to call them, and perform Stored Cross-Site Scripting attacks against logged in admin, as well as frontend users due to the lack of sanitisation and escaping in some parameters	5.4	More Details
CVE-2021-24842	The Bulk Datetime Change WordPress plugin before 1.12 does not enforce capability checks which allows users with Contributor roles to 1) list private post titles of other users and 2) change the posted date of other users' posts.	5.4	More Details
CVE-2021-44202	Stored cross-site scripting (XSS) was possible in activity details. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4020	janus-gateway is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-44203	Stored cross-site scripting (XSS) was possible in protection plan details. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035	5.4	More Details
CVE-2021-24918	The Smash Balloon Social Post Feed WordPress plugin before 4.0.1 did not have any privilege or nonce validation before saving the plugin's setting. As a result, any logged-in user on a vulnerable site could update the settings and store rogue JavaScript on each of its posts and pages.	5.4	More Details
CVE-2021-24883	The Popup Anything WordPress plugin before 2.0.4 does not escape the Link Text and Button Text fields of Popup, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks	5.4	More Details
CVE-2021-20843	Cross-site script inclusion vulnerability in the Web GUI of RTX830 Rev.15.02.17 and earlier, NVR510 Rev.15.01.18 and earlier, NVR700W Rev.15.00.19 and earlier, and RTX1210 Rev.14.01.38 and earlier allows a remote authenticated attacker to alter the settings of the product via a specially crafted web page.	5.4	More Details
CVE-2021-24927	The My Calendar WordPress plugin before 3.2.18 does not sanitise and escape the callback parameter of the mc_post_lookup AJAX action (available to any authenticated user) before outputting it back in the response, leading to a Reflected Cross-Site Scripting issue	5.4	More Details
CVE-2021-44225	In Keepalived through 2.2.4, the D-Bus policy does not sufficiently restrict the message destination, allowing any user to inspect and manipulate any property. This leads to access-control bypass in some situations in which an unrelated D-Bus system service has a settable (writable) property	5.4	More Details
CVE-2021-32061	S3Scanner before 2.0.2 allows Directory Traversal via a crafted bucket, as demonstrated by a <Key>../ substring in a ListBucketResult element.	5.3	More Details
CVE-2021-36327	Dell EMC Streaming Data Platform versions before 1.3 contain a Server Side Request Forgery Vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability to perform port scanning of internal networks and make HTTP requests to an arbitrary domain of the attacker's choice.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3553	A Server-Side Request Forgery (SSRF) vulnerability in the EPPUpdateService of Bitdefender Endpoint Security Tools allows an attacker to use the Endpoint Protection relay as a proxy for any remote host. This issue affects: Bitdefender Endpoint Security Tools versions prior to 6.6.27.390; versions prior to 7.1.2.33. Bitdefender Unified Endpoint for Linux versions prior to 6.2.21.160. Bitdefender GravityZone versions prior to 6.24.1-1.	5.3	More Details
CVE-2021-21707	In PHP versions 7.3.x below 7.3.33, 7.4.x below 7.4.26 and 8.0.x below 8.0.13, certain XML parsing functions, like simplexml_load_file(), URL-decode the filename passed to them. If that filename contains URL-encoded NUL character, this may cause the function to interpret this as the end of the filename, thus interpreting the filename differently from what the user intended, which may lead it to reading a different file than intended.	5.3	More Details
CVE-2021-3552	A Server-Side Request Forgery (SSRF) vulnerability in the EPPUpdateService component of Bitdefender Endpoint Security Tools allows an attacker to proxy requests to the relay server. This issue affects: Bitdefender Endpoint Security Tools versions prior to 6.6.27.390; versions prior to 7.1.2.33. Bitdefender GravityZone 6.24.1-1.	5.3	More Details
CVE-2021-42297	Windows 10 Update Assistant Elevation of Privilege Vulnerability	5.0	More Details
CVE-2021-25987	Hexo versions 0.0.1 to 5.4.0 are vulnerable against stored XSS. The post “body” and “tags” don’t sanitize malicious javascript during web page generation. Local unprivileged attacker can inject arbitrary code.	5.0	More Details
CVE-2021-43788	Nodebb is an open source Node.js based forum software. Prior to v1.18.5, a path traversal vulnerability was present that allowed users to access JSON files outside of the expected `languages/` directory. The vulnerability has been patched as of v1.18.5. Users are advised to upgrade as soon as possible.	5.0	More Details
CVE-2021-36843	Authenticated Stored Cross-Site Scripting (XSS) vulnerability discovered in WordPress Floating Social Media Icon plugin (versions <= 4.3.5) Social Media Configuration form. Requires high role user like admin.	4.8	More Details
CVE-2021-24768	The WP RSS Aggregator WordPress plugin before 4.19.2 does not properly sanitise and escape the URL to Blacklist field, allowing malicious HTML to be inserted by high privilege users even when the unfiltered_html capability is disallowed, which could lead to Cross-Site Scripting issues.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42365	The Asgaros Forums WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the name parameter found in the ~/admin/tables/admin-structure-table.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.15.13. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	4.8	More Details
CVE-2021-24899	The Media-Tags WordPress plugin through 3.2.0.2 does not sanitise and escape any of its Labels settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_htnl capability is disallowed.	4.8	More Details
CVE-2021-24811	The Shop Page WP WordPress plugin before 1.2.8 does not sanitise and escape some of the Product fields, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-25269	A local administrator could prevent the HMPA service from starting despite tamper protection using an unquoted service path vulnerability in the HMPA component of Sophos Intercept X Advanced and Sophos Intercept X Advanced for Server before version 2.0.23, as well as Sophos Exploit Prevention before version 3.8.3.	4.4	More Details
CVE-2021-42122	Insufficient Input Validation in Web Applications operating on Business-DNA Solutions GmbH’s TopEase® Platform Version <= 7.1.27 on an object’s attributes with numeric format allows an authenticated remote attacker with Object Modification privileges to insert an unexpected format, which makes the affected attribute non-editable.	4.3	More Details
CVE-2021-42116	Incorrect Access Control in Web Applications operating on Business-DNA Solutions GmbH’s TopEase® Platform Version <= 7.1.27 allows an authenticated remote attacker to view the Shape Editor and Settings, which are functionality for higher privileged users, via identifying said components in the front-end source code or other means.	4.3	More Details
CVE-2021-4026	bookstack is vulnerable to Improper Access Control	4.3	More Details
CVE-2021-24749	The URL Shortify WordPress plugin before 1.5.1 does not have CSRF check in place when bulk-deleting links or groups, which could allow attackers to make a logged in admin delete arbitrary link and group via a CSRF attack.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42121	Insufficient Input Validation in Web Applications operating on Business-DNA Solutions GmbH's TopEase® Platform Version <= 7.1.27 on an object's date attribute(s) allows an authenticated remote attacker with Object Modification privileges to insert an unexpected format into date fields, which leads to breaking the object page that the date field is present.	4.3	More Details
CVE-2021-3802	A vulnerability found in udisks2. This flaw allows an attacker to input a specially crafted image file/USB leading to kernel panic. The highest threat from this vulnerability is to system availability.	4.2	More Details
CVE-2021-43221	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	4.2	More Details
CVE-2021-42117	Insufficient Input Validation in Web Applications operating on Business-DNA Solutions GmbH's TopEase® Platform Version <= 7.1.27 allows an authenticated remote attacker with Object Modification privileges to insert arbitrary HTML without code execution.	3.5	More Details
CVE-2021-43220	Microsoft Edge for iOS Spoofing Vulnerability	3.1	More Details
CVE-2021-42308	Microsoft Edge (Chromium-based) Spoofing Vulnerability	3.1	More Details
CVE-2021-43320	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-41244. Reason: This candidate is a reservation duplicate of CVE-2021-41244. Notes: All CVE users should reference CVE-2021-41244 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details