SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 10 March 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-2021-27314	SQL injection in admin.php in doctor appointment system 1.0 allows an unauthenticated attacker to insert malicious SQL queries via username parameter at login page.	9.8	More Details
CVE-2020-8298	fs-path node module before 0.0.25 is vulnerable to command injection by way of user-supplied inputs via the `copy`, `copySync`, `remove`, and `removeSync` methods.	9.8	More Details
CVE-2021-27964	SonLogger before 6.4.1 is affected by Unauthenticated Arbitrary File Upload. An attacker can send a POST request to /Config/SaveUploadedHotspotLogoFile without any authentication or session header. There is no check for the file extension or content of the uploaded file.	9.8	More Details
CVE-2021-27965	The MsIo64.sys driver before 1.1.19.1016 in MSI Dragon Center before 2.0.98.0 has a buffer overflow that allows privilege escalation via a crafted 0x80102040, 0x80102044, 0x80102050, or 0x80102054 IOCTL request.	9.8	More Details
CVE-2020-29658	Zoho ManageEngine Application Control Plus before 100523 has an insecure SSL configuration setting for Nginx, leading to Privilege Escalation.	9.8	More Details
CVE-2021-28027	An issue was discovered in the bam crate before 0.1.3 for Rust. There is an integer underflow and out-of-bounds write during the loading of a bgzip block.	9.8	More Details
CVE-2021-28028	An issue was discovered in the toodee crate before 0.3.0 for Rust. Row insertion can cause a double free upon an iterator panic.	9.8	More Details
CVE-2021-28031	An issue was discovered in the scratchpad crate before 1.3.1 for Rust. The move_elements function can have a double-free upon a panic in a user-provided f function.	9.8	More Details
CVE-2021-28032	An issue was discovered in the nano_arena crate before 0.5.2 for Rust. There is an aliasing violation in split_at because two mutable references can exist for the same element, if Borrow<Idx> behaves in certain ways. This can have a resultant out-of-bounds write or use-after-free.	9.8	More Details
CVE-2021-28033	An issue was discovered in the byte_struct crate before 0.6.1 for Rust. There can be a drop of uninitialized memory if a certain deserialization method panics.	9.8	More Details
CVE-2021-28034	An issue was discovered in the stack_dst crate before 0.6.1 for Rust. Because of the push_inner behavior, a double free can occur upon a val.clone() panic.	9.8	More Details
CVE-2021-28035	An issue was discovered in the stack_dst crate before 0.6.1 for Rust. Because of the push_inner behavior, a drop of uninitialized memory can occur upon a val.clone() panic.	9.8	More Details
CVE-2021-28037	An issue was discovered in the internment crate before 0.4.2 for Rust. There is a data race that can cause memory corruption because of the unconditional implementation of Sync for Intern<T>.	9.8	More Details
CVE-2021-3420	A flaw was found in newlib in versions prior to 4.0.0. Improper overflow validation in the memory allocation functions mEMALIGn, pvALLOc, nano_memalign, nano_valloc, nano_pvalloc could case an integer overflow, leading to an allocation of a small buffer and then to a heap-based buffer overflow.	9.8	More Details
CVE-2021-27581	The Blog module in Kentico CMS 5.5 R2 build 5.5.3996 allows SQL injection via the tagname parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21484	LDAP authentication in SAP HANA Database version 2.0 can be bypassed if the attached LDAP directory server is configured to enable unauthenticated bind.	9.8	More Details
CVE-2021-25915	Prototype pollution vulnerability in 'changeset' versions 0.0.1 through 0.2.5 allows an attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2021-26293	An issue was discovered in AfterLogic Aurora through 8.5.3 and WebMail Pro through 8.5.3, when DAV is enabled. They allow directory traversal to create new files (such as an executable file under the web root). This is related to DAVServer.php in 8.x and DAV/Server.php in 7.x.	9.8	More Details
CVE-2021-28119	Twinkle Tray (aka twinkle-tray) through 1.13.3 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 API.	9.8	More Details
CVE-2020-35636	A code execution vulnerability exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1 in Nef_S2/SNC_io_parser.h SNC_io_parser::read_sface() sfh->volume() OOB read. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger this vulnerability.	9.8	More Details
CVE-2020-35628	A code execution vulnerability exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser::read_sloop() slh->incident_sface. An attacker can provide malicious input to trigger this vulnerability.	9.8	More Details
CVE-2020-28636	A code execution vulnerability exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser::read_sloop() slh->twin() An attacker can provide malicious input to trigger this vulnerability.	9.8	More Details
CVE-2020-28601	A code execution vulnerability exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. An oob read vulnerability exists in Nef_2/PM_io_parser.h PM_io_parser::read_vertex() Face_of[] OOB read. An attacker can provide malicious input to trigger this vulnerability.	9.8	More Details
CVE-2021-25315	CWE - CWE-287: Improper Authentication vulnerability in SUSE Linux Enterprise Server 15 SP 3; openSUSE Tumbleweed allows local attackers to execute arbitrary code via salt without the need to specify valid credentials. This issue affects: SUSE Linux Enterprise Server 15 SP 3 salt versions prior to 3002.2-3. openSUSE Tumbleweed salt version 3002.2-2.1 and prior versions. This issue affects: SUSE Linux Enterprise Server 15 SP 3 salt versions prior to 3002.2-3. openSUSE Tumbleweed salt version 3002.2-2.1 and prior versions.	9.8	More Details
CVE-2021-23344	The package total.js before 3.4.8 are vulnerable to Remote Code Execution (RCE) via set.	9.8	More Details
CVE-2020-24914	A PHP object injection bug in profile.php in qcubed (all versions including 3.1.1) unserializes the untrusted data of the POST-variable "strProfileData" and allows an unauthenticated attacker to execute code via a crafted POST request.	9.8	More Details
CVE-2020-24913	A SQL injection vulnerability in qcubed (all versions including 3.1.1) in profile.php via the strQuery parameter allows an unauthenticated attacker to access the database by injecting SQL code via a crafted POST request.	9.8	More Details
CVE-2021-27215	An issue was discovered in genua genugate before 9.0 Z p19, 9.1.x through 9.6.x before 9.6 p7, and 10.x before 10.1 p4. The Web Interfaces (Admin, Userweb, Sidechannel) can use different methods to perform the authentication of a user. A specific authentication method during login does not check the provided data (when a certain manipulation occurs) and returns OK for any authentication request. This allows an attacker to login to the admin panel as a user of his choice, e.g., the root user (with highest privileges) or even a non-existing user.	9.8	More Details
CVE-2021-22681	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800.	9.8	More Details
CVE-2021-21978	VMware View Planner 4.x prior to 4.6 Security Patch 1 contains a remote code execution vulnerability. Improper input validation and lack of authorization leading to arbitrary file upload in logupload web application. An unauthorized attacker with network access to View Planner Harness could upload and execute a specially crafted file leading to remote code execution within the logupload container.	9.8	More Details
CVE-2020-29047	The wp-hotel-booking plugin through 1.10.2 for WordPress allows remote attackers to execute arbitrary code because of an unserialize operation on the thimpress_hotel_booking_1 cookie in load in includes/class-wphb-sessions.php.	9.8	More Details
CVE-2020-29020	Improper Access Control vulnerability in web service of Secomea SiteManager allows remote attacker to access the web UI from the internet using the configured credentials. This issue affects: Secomea SiteManager All versions prior to 9.4.620527004 on Hardware.	9.1	More Details
CVE-2021-27078	Microsoft Exchange Server Remote Code Execution Vulnerability	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27931	LumisXP (aka Lumis Experience Platform) before 10.0.0 allows unauthenticated blind XXE via an API request to PageControllerXml.jsp. One can send a request crafted with an XXE payload and achieve outcomes such as reading local server files or denial of service.	9.1	More Details
CVE-2021-26705	An issue was discovered in SquareBox CatDV Server through 9.2. An attacker can invoke sensitive RMI methods such as getConnections without authentication, the results of which can be used to generate valid authentication tokens. These tokens can then be used to invoke administrative tasks within the application, such as disclosing password hashes.	9.1	More Details
CVE-2020-28050	Zoho ManageEngine Desktop Central before build 10.0.647 allows a single authentication secret from multiple agents to communicate with the server.	9.1	More Details
CVE-2021-26855	Microsoft Exchange Server Remote Code Execution Vulnerability	9.1	More Details
CVE-2021-23127	An issue was discovered in Joomla! 3.2.0 through 3.9.24. Usage of an insufficient length for the 2FA secret accoring to RFC 4226 of 10 bytes vs 20 bytes.	9.1	More Details
CVE-2021-23128	An issue was discovered in Joomla! 3.2.0 through 3.9.24. The core shipped but unused randval implementation within FOF (FOFEncryptRandval) used an potential insecure implemetation. That has now been replaced with a call to 'random_bytes()' and its backport that is shipped within random_compat.	9.1	More Details
CVE-2021-26412	Microsoft Exchange Server Remote Code Execution Vulnerability	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-21159	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21480	SAP MII allows users to create dashboards and save them as JSP through the SSCE (Self Service Composition Environment). An attacker can intercept a request to the server, inject malicious JSP code in the request and forward to server. When this dashboard is opened by users having at least SAP_XMII Developer role, malicious content in the dashboard gets executed, leading to remote code execution in the server, which allows privilege escalation. The malicious JSP code can contain certain OS commands, through which an attacker can read sensitive files in the server, modify files or even delete contents in the server thus compromising the confidentiality, integrity and availability of the server hosting the SAP MII application. Also, an attacker authenticated as a developer can use the application to upload and execute a file which will permit them to execute operating systems commands completely compromising the server hosting the application.	8.8	More Details
CVE-2021-21190	Uninitialized data in PDFium in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.	8.8	More Details
CVE-2021-21486	SAP Enterprise Financial Services versions, 101, 102, 103, 104, 105, 600, 603, 604, 605, 606, 616, 617, 618, 800, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	8.8	More Details
CVE-2021-21487	SAP Payment Engine version 500, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	8.8	More Details
CVE-2021-21160	Heap buffer overflow in WebAudio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-20076	Tenable.sc and Tenable.sc Core versions 5.13.0 through 5.17.0 were found to contain a vulnerability that could allow an authenticated, unprivileged user to perform Remote Code Execution (RCE) on the Tenable.sc server via Hypertext Preprocessor unserialization.	8.8	More Details
CVE-2021-21161	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21162	Use after free in WebRTC in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21165	Data race in audio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21166	Data race in audio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21167	Use after free in bookmarks in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21169	Out of bounds memory access in V8 in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	8.8	More Details
CVE-2021-21174	Inappropriate implementation in Referrer in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	8.8	More Details
CVE-2020-24036	PHP object injection in the Ajax endpoint of the backend in ForkCMS below version 5.8.3 allows an authenticated remote user to execute malicious code.	8.8	More Details
CVE-2021-27927	In Zabbix from 4.0.x before 4.0.28rc1, 5.0.0alpha1 before 5.0.10rc1, 5.2.x before 5.2.6rc1, and 5.4.0alpha1 before 5.4.0beta2, the CControllerAuthenticationUpdate controller lacks a CSRF protection mechanism. The code inside this controller calls diableSIDValidation inside the init() method. An attacker doesn't have to know Zabbix user login credentials, but has to know the correct Zabbix URL and contact information of an existing user with sufficient privileges.	8.8	More Details
CVE-2020-13558	A code execution vulnerability exists in the AudioSourceProviderGStreamer functionality of Webkit WebKitGTK 2.30.1. A specially crafted web page can lead to a use after free.	8.8	More Details
CVE-2021-21179	Use after free in Network Internals in Google Chrome on Linux prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21180	Use after free in tab search in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21481	The MigrationService, which is part of SAP NetWeaver versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not perform an authorization check. This might allow an unauthorized attacker to access configuration objects, including such that grant administrative privileges. This could result in complete compromise of system confidentiality, integrity, and availability.	8.8	More Details
CVE-2021-21188	Use after free in Blink in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21506	PowerScale OneFS 8.1.2,8.2.2 and 9.1.0 contains an improper input sanitization issue in its API handler. An un-authtenticated with ISI_PRIV_SYS_SUPPORT and ISI_PRIV_LOGIN_PAPI privileges could potentially exploit this vulnerability, leading to potential privileges escalation.	8.8	More Details
CVE-2021-27254	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R7800. Authentication is not required to exploit this vulnerability. The specific flaw exists within the apply_save.cgi endpoint. This issue results from the use of hard-coded encryption key. An attacker can leverage this vulnerability to execute arbitrary code in the context of root. Was ZDI-CAN-12287.	8.8	More Details
CVE-2020-27575	Maxum Rumpus 8.2.13 and 8.2.14 is affected by a command injection vulnerability. The web administration contains functionality in which administrators are able to manage users. The edit users form contains a parameter vulnerable to command injection due to insufficient validation.	8.8	More Details
CVE-2020-27574	Maxum Rumpus 8.2.13 and 8.2.14 is affected by cross-site request forgery (CSRF). If an authenticated user visits a malicious page, unintended actions could be performed in the web application as the authenticated user.	8.8	More Details
CVE-2021-26960	A remote unauthenticated cross-site request forgery (csrf) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the AirWave web-based management interface could allow an unauthenticated remote attacker to conduct a CSRF attack against a vulnerable system. A successful exploit would consist of an attacker persuading an authorized user to follow a malicious link, resulting in arbitrary actions being carried out with the privilege level of the targeted user.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26814	Wazuh API in Wazuh from 4.0.0 to 4.0.3 allows authenticated users to execute arbitrary code with administrative privileges via /manager/files URI. An authenticated user to the service may exploit incomplete input validation on the /manager/files API to inject arbitrary code within the API service script.	8.8	More Details
CVE-2021-26961	A remote unauthenticated cross-site request forgery (csrf) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the AirWave web-based management interface could allow an unauthenticated remote attacker to conduct a CSRF attack against a vulnerable system. A successful exploit would consist of an attacker persuading an authorized user to follow a malicious link, resulting in arbitrary actions being carried out with the privilege level of the targeted user.	8.8	More Details
CVE-2021-27256	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R7800 firmware version 1.0.2.76. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of the rc_service parameter provided to apply_save.cgi. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-12355.	8.8	More Details
CVE-2021-27255	This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR R7800 firmware version 1.0.2.76. Authentication is not required to exploit this vulnerability. The specific flaw exists within the refresh_status.aspx endpoint. The issue results from a lack of authentication required to start a service on the server. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-12360.	8.8	More Details
CVE-2020-10519	A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration of the underlying parsers used by GitHub Pages were not sufficiently restricted and made it possible to execute commands on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22.7 and was fixed in 2.22.7, 2.21.15, and 2.20.24. The underlying issues contributing to this vulnerability were identified through the GitHub Security Bug Bounty program.	8.8	More Details
CVE-2021-21329	RATCF is an open-source framework for hosting Cyber-Security Capture the Flag events. In affected versions of RATCF users with multi factor authentication enabled are able to log in without a valid token. This is fixed in commit cebb67b.	8.7	More Details
CVE-2021-23352	This affects the package madge before 4.0.1. It is possible to specify a custom Graphviz path via the graphVizPath option parameter which when the .image(), .svg() or .dot() functions are called, is executed by the childprocess.exec function.	8.6	More Details
CVE-2020-29134	The TOTVS Fluig platform allows path traversal through the parameter "file = .. /" encoded in base64. This affects all versions Fluig Lake 1.7.0, Fluig 1.6.5 and Fluig 1.6.4	8.6	More Details
CVE-2020-29032	Upload of Code Without Integrity Check vulnerability in firmware archive of Secomea GateManager allows authenticated attacker to execute malicious code on server. This issue affects: Secomea GateManager all versions prior to 9.4.621054022	8.4	More Details
CVE-2020-25632	A flaw was found in grub2 in versions prior to 2.06. The rmmod implementation allows the unloading of a module used as a dependency without checking if any other dependent module is still loaded leading to a use-after-free scenario. This could allow arbitrary code to be executed or a bypass of Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	8.2	More Details
CVE-2021-27963	SonLogger before 6.4.1 is affected by user creation with any user permissions profile (e.g., SuperAdmin). An anonymous user can send a POST request to /User/saveUser without any authentication or session header.	8.2	More Details
CVE-2021-20233	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	8.2	More Details
CVE-2020-5148	SonicWall SSO-agent default configuration uses NetAPI to probe the associated IP's in the network, this client probing method allows a potential attacker to capture the password hash of the privileged user and potentially forces the SSO Agent to authenticate allowing an attacker to bypass firewall access controls.	8.2	More Details
CVE-2021-21172	Insufficient policy enforcement in File System API in Google Chrome on Windows prior to 89.0.4389.72 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.	8.1	More Details
CVE-2020-28502	This affects the package xmlhttprequest before 1.7.0; all versions of package xmlhttprequest-ssl. Provided requests are sent synchronously (async=False on xhr.open), malicious user input flowing into xhr.send could result in arbitrary code being injected and run.	8.1	More Details
CVE-2019-18629	Xerox AltaLink B8045/B8055/B8065/B8075/B8090 and C8030/C8035/C8045/C8055/C8070 multifunction printers with software releases before 101.00x.099.28200 allow an attacker to execute an unwanted binary during a exploited clone install. This requires creating a clone file and signing that file with a compromised private key.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29030	Cross-Site Request Forgery (CSRF) vulnerability in web GUI of Secomea GateManager allows an attacker to execute malicious code. This issue affects: Secomea GateManager All versions prior to 9.4.	8.1	More Details
CVE-2021-27098	In SPIRE 0.8.1 through 0.8.4 and before versions 0.9.4, 0.10.2, 0.11.3 and 0.12.1, specially crafted requests to the FetchX509SVID RPC of SPIRE Server's Legacy Node API can result in the possible issuance of an X.509 certificate with a URI SAN for a SPIFFE ID that the agent is not authorized to distribute. Proper controls are in place to require that the caller presents a valid agent certificate that is already authorized to issue at least one SPIFFE ID, and the requested SPIFFE ID belongs to the same trust domain, prior to being able to trigger this vulnerability. This issue has been fixed in SPIRE versions 0.8.5, 0.9.4, 0.10.2, 0.11.3 and 0.12.1.	8.1	More Details
CVE-2009-20001	An issue was discovered in MantisBT before 2.24.5. It associates a unique cookie string with each user. This string is not reset upon logout (i.e., the user session is still considered valid and active), allowing an attacker who somehow gained access to a user's cookie to login as them.	8.1	More Details
CVE-2021-22863	An improper access control vulnerability was identified in the GitHub Enterprise Server GraphQL API that allowed authenticated users of the instance to modify the maintainer collaboration permission of a pull request without proper authorization. By exploiting this vulnerability, an attacker would be able to gain access to head branches of pull requests opened on repositories of which they are a maintainer. Forking is disabled by default for organization owned private repositories and would prevent this vulnerability. Additionally, branch protections such as required pull request reviews or status checks would prevent unauthorized commits from being merged without further review or validation. This vulnerability affected all versions of GitHub Enterprise Server since 2.12.22 and was fixed in versions 2.20.24, 2.21.15, 2.22.7 and 3.0.1. This vulnerability was reported via the GitHub Bug Bounty program.	8.1	More Details
CVE-2021-21300	Git is an open-source distributed revision control system. In affected versions of Git a specially crafted repository that contains symbolic links as well as files using a clean/smudge filter such as Git LFS, may cause just-checked out script to be executed while cloning onto a case-insensitive file system such as NTFS, HFS+ or APFS (i.e. the default file systems on Windows and macOS). Note that clean/smudge filters have to be configured for that. Git for Windows configures Git LFS by default, and is therefore vulnerable. The problem has been patched in the versions published on Tuesday, March 9th, 2021. As a workaound, if symbolic link support is disabled in Git (e.g. via `git config --global core.symlinks false`), the described attack won't work. Likewise, if no clean/smudge filters such as Git LFS are configured globally (i.e. _before_ cloning), the attack is foiled. As always, it is best to avoid cloning repositories from untrusted sources. The earliest impacted version is 2.14.2. The fix versions are: 2.30.1, 2.29.3, 2.28.1, 2.27.1, 2.26.3, 2.25.5, 2.24.4, 2.23.4, 2.22.5, 2.21.4, 2.20.5, 2.19.6, 2.18.5, 2.17.62.17.6.	8.0	More Details
CVE-2021-23273	The Spotfire client component of TIBCO Software Inc.'s TIBCO Spotfire Analyst, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Desktop, and TIBCO Spotfire Server contains a vulnerability that theoretically allows a low privileged attacker with network access to execute a stored Cross Site Scripting (XSS) attack on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analyst: versions 10.3.3 and below, versions 10.10.0, 10.10.1, and 10.10.2, versions 10.7.0, 10.8.0, 10.9.0, 11.0.0, and 11.1.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 11.1.0 and below, TIBCO Spotfire Desktop: versions 10.3.3 and below, versions 10.10.0, 10.10.1, and 10.10.2, versions 10.7.0, 10.8.0, 10.9.0, 11.0.0, and 11.1.0, and TIBCO Spotfire Server: versions 10.3.11 and below, versions 10.10.0, 10.10.1, 10.10.2, and 10.10.3, versions 10.7.0, 10.8.0, 10.8.1, 10.9.0, 11.0.0, and 11.1.0.	8.0	More Details
CVE-2021-27587	When a user opens manipulated Jupiter Tessellation (.JT) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	7.8	More Details
CVE-2021-22638	Fatek FvDesigner Version 1.5.76 and prior is vulnerable to an out-of-bounds read while processing project files, allowing an attacker to craft a special project file that may permit arbitrary code execution.	7.8	More Details
CVE-2020-35524	A heap-based buffer overflow flaw was found in libtiff in the handling of TIFF images in libtiff's TIFF2PDF tool. A specially crafted TIFF file can lead to arbitrary code execution. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	7.8	More Details
CVE-2021-20268	An out-of-bounds access flaw was found in the Linux kernel's implementation of the eBPF code verifier in the way a user running the eBPF script calls dev_map_init_map or sock_map_alloc. This flaw allows a local user to crash the system or possibly escalate their privileges. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	7.8	More Details
CVE-2021-27592	When a user opens manipulated Universal 3D (.U3D) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	7.8	More Details
CVE-2021-27591	When a user opens manipulated Portable Document Format (.PDF) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	7.8	More Details
CVE-2021-27590	When a user opens manipulated Tag Image File Format (.TIFF) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27588	When a user opens manipulated HPGL format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	7.8	More Details
CVE-2021-27585	When a user opens manipulated Computer Graphics Metafile (.CGM) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	7.8	More Details
CVE-2021-27586	When a user opens manipulated Interchange File Format (.IFF) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	7.8	More Details
CVE-2021-28026	jpeg-xl v0.3.2 is affected by a heap buffer overflow in /lib/jxl/coeff_order.cc ReadPermutation. When decoding a malicous jxl file using djxl, an attacker can trigger arbitrary code execution or a denial of service.	7.8	More Details
CVE-2020-13554	An exploitable local privilege elevation vulnerability exists in the file system permissions of Advantech WebAccess/SCADA 9.0.1 installation. In webvrpcs Run Key Privilege Escalation in installation folder of WebAccess, an attacker can either replace binary or loaded modules to execute code with NT SYSTEM privilege.	7.8	More Details
CVE-2020-35523	An integer overflow flaw was found in libtiff that exists in the tif_getimage.c file. This flaw allows an attacker to inject and execute arbitrary code when a user opens a crafted TIFF file. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	7.8	More Details
CVE-2021-21503	PowerScale OneFS 8.1.2,8.2.2 and 9.1.0 contains an improper input sanitization issue in a command. The Compadmin user could potentially exploit this vulnerability, leading to potential privileges escalation.	7.8	More Details
CVE-2021-3403	In ytnef 1.9.3, the TNEFSubjectHandler function in lib/ytnef.c allows remote attackers to cause a denial-of-service (and potentially code execution) due to a double free which can be triggered via a crafted file.	7.8	More Details
CVE-2021-3404	In ytnef 1.9.3, the SwapWord function in lib/ytnef.c allows remote attackers to cause a denial-of-service (and potentially code execution) due to a heap buffer overflow which can be triggered via a crafted file.	7.8	More Details
CVE-2021-26857	Microsoft Exchange Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-22662	A use after free issue has been identified in Fatek FvDesigner Version 1.5.76 and prior in the way the application processes project files, allowing an attacker to craft a special project file that may permit arbitrary code execution.	7.8	More Details
CVE-2021-27589	When a user opens manipulated Scalable Vector Graphics (.SVG) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	7.8	More Details
CVE-2021-22683	Fatek FvDesigner Version 1.5.76 and prior is vulnerable to an out-of-bounds write while processing project files, allowing an attacker to craft a special project file that may permit arbitrary code execution.	7.8	More Details
CVE-2021-22666	Fatek FvDesigner Version 1.5.76 and prior is vulnerable to a stack-based buffer overflow while project files are being processed, allowing an attacker to craft a special project file that may permit arbitrary code execution.	7.8	More Details
CVE-2020-27225	In versions 4.18 and earlier of the Eclipse Platform, the Help Subsystem does not authenticate active help requests to the local help web server, allowing an unauthenticated local attacker to issue active help commands to the associated Eclipse Platform process or Eclipse Rich Client Platform process.	7.8	More Details
CVE-2021-27365	An issue was discovered in the Linux kernel through 5.11.3. Certain iSCSI data structures do not have appropriate length constraints or checks, and can exceed the PAGE_SIZE value. An unprivileged user can send a Netlink message that is associated with iSCSI, and has a length up to the maximum length of a Netlink message.	7.8	More Details
CVE-2020-23967	Dr.Web Security Space versions 11 and 12 allow elevation of privilege for local users without administrative privileges to NT AUTHORITY\SYSTEM due to insufficient control during autoupdate.	7.8	More Details
CVE-2021-26858	Microsoft Exchange Server Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28042	Deutsche Post Mailoptimizer 4.3 before 2020-11-09 allows Directory Traversal via a crafted ZIP archive to the Upload feature or the MO Connect component. This can lead to remote code execution.	7.8	More Details
CVE-2021-22670	An uninitialized pointer may be exploited in Fatek FvDesigner Version 1.5.76 and prior while the application is processing project files, allowing an attacker to craft a special project file that may permit arbitrary code execution.	7.8	More Details
CVE-2021-27065	Microsoft Exchange Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-21362	MinIO is an open-source high performance object storage service and it is API compatible with Amazon S3 cloud storage service. In MinIO before version RELEASE.2021-03-04T00-53-13Z it is possible to bypass a readOnly policy by creating a temporary 'mc share upload' URL. Everyone is impacted who uses MinIO multi-users. This is fixed in version RELEASE.2021-03-04T00-53-13Z. As a workaround, one can disable uploads with `Content-Type: multipart/form-data` as mentioned in the S3 API RESTObjectPOST docs by using a proxy in front of MinIO.	7.7	More Details
CVE-2021-21326	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. In GLPI before version 9.5.4 it is possible to create tickets for another user with self-service interface without delegatee systems enabled. This is fixed in version 9.5.4.	7.7	More Details
CVE-2020-25647	A flaw was found in grub2 in versions prior to 2.06. During USB device initialization, descriptors are read with very little bounds checking and assumes the USB device is providing sane values. If properly exploited, an attacker could trigger memory corruption leading to arbitrary code execution allowing a bypass of the Secure Boot mechanism. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.6	More Details
CVE-2021-22883	Node.js before 10.24.0, 12.21.0, 14.16.0, and 15.10.0 is vulnerable to a denial of service attack when too many connection attempts with an 'unknownProtocol' are established. This leads to a leak of file descriptors. If a file descriptor limit is configured on the system, then the server is unable to accept new connections and prevent the process also from opening, e.g. a file. If no file descriptor limit is configured, then this lead to an excessive memory usage and cause the system to run out of memory.	7.5	More Details
CVE-2021-27921	Pillow before 8.1.1 allows attackers to cause a denial of service (memory consumption) because the reported size of a contained image is not properly checked for a BLP container, and thus an attempted memory allocation can be very large.	7.5	More Details
CVE-2021-20276	A flaw was found in privoxy before 3.0.32. Invalid memory access with an invalid pattern passed to pcre_compile() may lead to denial of service.	7.5	More Details
CVE-2021-20275	A flaw was found in privoxy before 3.0.32. A invalid read of size two may occur in chunked_body_is_complete() leading to denial of service.	7.5	More Details
CVE-2021-20274	A flaw was found in privoxy before 3.0.32. A crash may occur due a NULL-pointer dereference when the socks server misbehaves.	7.5	More Details
CVE-2021-20273	A flaw was found in privoxy before 3.0.32. A crash can occur via a crafted CGI request if Privoxy is toggled off.	7.5	More Details
CVE-2021-20272	A flaw was found in privoxy before 3.0.32. An assertion failure could be triggered with a crafted CGI request leading to server crash.	7.5	More Details
CVE-2021-27935	An issue was discovered in AdGuard before 0.105.2. An attacker able to get the user's cookie is able to bruteforce their password offline, because the hash of the password is stored in the cookie.	7.5	More Details
CVE-2020-35296	ThinkAdmin v6 has default administrator credentials, which allows attackers to gain unrestricted administratior dashboard access.	7.5	More Details
CVE-2021-23132	An issue was discovered in Joomla! 3.0.0 through 3.9.24. com_media allowed paths that are not intended for image uploads	7.5	More Details
CVE-2021-23131	An issue was discovered in Joomla! 3.2.0 through 3.9.24. Missing input validation within the template manager.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28466	This affects all versions of package github.com/nats-io/nats-server/server. Untrusted accounts are able to crash the server using configs that represent a service export/import cycles. Disclaimer from the maintainers: Running a NATS service which is exposed to untrusted users presents a heightened risk. Any remote execution flaw or equivalent seriousness, or denial-of-service by unauthenticated users, will lead to prompt releases by the NATS maintainers. Fixes for denial of service issues with no threat of remote execution, when limited to account holders, are likely to just be committed to the main development branch with no special attention. Those who are running such services are encouraged to build regularly from git.	7.5	More Details
CVE-2019-18630	On Xerox AltaLink B8045/B8055/B8065/B8075/B8090 and C8030/C8035/C8045/C8055/C8070 multifunction printers with software releases before 101.00x.099.28200, portions of the drive containing executable code were not encrypted thus leaving it open to potential cryptographic information disclosure.	7.5	More Details
CVE-2021-22884	Node.js before 10.24.0, 12.21.0, 14.16.0, and 15.10.0 is vulnerable to DNS rebinding attacks as the whitelist includes “localhost6”. When “localhost6” is not present in /etc/hosts, it is just an ordinary domain that is resolved via DNS, i.e., over network. If the attacker controls the victim's DNS server or can spoof its responses, the DNS rebinding protection can be bypassed by using the “localhost6” domain. As long as the attacker uses the “localhost6” domain, they can still apply the attack described in CVE-2018-7160.	7.5	More Details
CVE-2021-26813	markdown2 >=1.0.1.18, fixed in 2.4.0, is affected by a regular expression denial of service vulnerability. If an attacker provides a malicious string, it can make markdown2 processing difficult or delayed for an extended period of time.	7.5	More Details
CVE-2020-14372	A flaw was found in grub2 in versions prior to 2.06, where it incorrectly enables the usage of the ACPI command when Secure Boot is enabled. This flaw allows an attacker with privileged access to craft a Secondary System Description Table (SSDT) containing code to overwrite the Linux kernel lockdown variable content directly into memory. The table is further loaded and executed by the kernel, defeating its Secure Boot lockdown and allowing the attacker to load unsigned code. The highest threat from this vulnerability is to data confidentiality and integrity, as well as system availability.	7.5	More Details
CVE-2020-28952	An issue was discovered on Athom Homey and Homey Pro devices before 5.0.0. ZigBee hub devices should generate a unique Standard Network Key that is then exchanged with all enrolled devices so that all inter-device communication is encrypted. However, the cited Athom products use another widely known key that is designed for testing purposes: "01030507090b0d0f00020406080a0c0d" (the decimal equivalent of 1 3 5 7 9 11 13 15 0 2 4 6 8 10 12 13), which is human generated and static across all issued devices.	7.5	More Details
CVE-2021-28040	An issue was discovered in OSSEC 3.6.0. An uncontrolled recursion vulnerability in os_xml.c occurs when a large number of opening and closing XML tags is used. Because recursion is used in _ReadElem without restriction, an attacker can trigger a segmentation fault once unmapped memory is reached.	7.5	More Details
CVE-2021-28029	An issue was discovered in the toodee crate before 0.3.0 for Rust. The row-insertion feature allows attackers to read the contents of uninitialized memory locations.	7.5	More Details
CVE-2020-27779	A flaw was found in grub2 in versions prior to 2.06. The cutmem command does not honor secure boot locking allowing an privileged attacker to remove address ranges from memory creating an opportunity to circumvent SecureBoot protections after proper triage about grub's memory layout. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.5	More Details
CVE-2021-26788	Oryx Embedded CycloneTCP 1.7.6 to 2.0.0, fixed in 2.0.2, is affected by incorrect input validation, which may cause a denial of service (DoS). To exploit the vulnerability, an attacker needs to have TCP connectivity to the target system. Receiving a maliciously crafted TCP packet from an unauthenticated endpoint is sufficient to trigger the bug.	7.5	More Details
CVE-2021-20442	IBM Security Verify Bridge contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 196618.	7.5	More Details
CVE-2020-4695	IBM API Connect V10 is impacted by insecure communications during database replication. As the data replication happens over insecure communication channels, an attacker can view unencrypted data leading to a loss of confidentiality.	7.5	More Details
CVE-2021-28036	An issue was discovered in the quinn crate before 0.7.0 for Rust. It may have invalid memory access for certain versions of the standard library because it relies on a direct cast of std::net::SocketAddrV4 and std::net::SocketAddrV6 data structures.	7.5	More Details
CVE-2021-27922	Pillow before 8.1.1 allows attackers to cause a denial of service (memory consumption) because the reported size of a contained image is not properly checked for an ICNS container, and thus an attempted memory allocation can be very large.	7.5	More Details
CVE-2020-36255	An issue was discovered in IdentityModel (aka ScottBrady.IdentityModel) before 1.3.0. The Branca implementation allows an attacker to modify and forge authentication tokens.	7.5	More Details
CVE-2021-28030	An issue was discovered in the truetype crate before 0.30.1 for Rust. Attackers can read the contents of uninitialized memory locations via a user-provided Read operation within Tape::take_bytes.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27923	Pillow before 8.1.1 allows attackers to cause a denial of service (memory consumption) because the reported size of a contained image is not properly checked for an ICO container, and thus an attempted memory allocation can be very large.	7.5	More Details
CVE-2021-26294	An issue was discovered in AfterLogic Aurora through 7.7.9 and WebMail Pro through 7.7.9. They allow directory traversal to read files (such as a data/settings/settings.xml file containing admin panel credentials), as demonstrated by dav/server.php/files/personal/%2e%2e when using the caldav_public_user account (with caldav_public_user as its password).	7.5	More Details
CVE-2020-28597	A predictable seed vulnerability exists in the password reset functionality of Epignosis EfrontPro 5.2.21. By predicting the seed it is possible to generate the correct password reset 1-time token. An attacker can visit the password reset supplying the password reset token to reset the password of an account of their choice.	7.5	More Details
CVE-2021-21354	Pollbot is open source software which "frees its human masters from the toilsome task of polling for the state of things during the Firefox release process." In Pollbot before version 1.4.4 there is an open redirection vulnerability in the path of "https://pollbot.services.mozilla.com/". An attacker can redirect anyone to malicious sites. To Reproduce type in this URL: "https://pollbot.services.mozilla.com//evil.com/". Affected versions will redirect to that website when you inject a payload like "//evil.com/". This is fixed in version 1.4.4.	7.4	More Details
CVE-2020-29029	Improper Input Validation, Cross-site Scripting (XSS) vulnerability in Web GUI of Secomea GateManager allows an attacker to execute arbitrary javascript code. This issue affects: Secomea GateManager all versions prior to 9.4.	7.3	More Details
CVE-2021-21979	In Bitnami Containers, all Laravel container versions prior to: 6.20.0-debian-10-r107 for Laravel 6, 7.30.1-debian-10-r108 for Laravel 7 and 8.5.11-debian-10-r0 for Laravel 8, the file /tmp/app/.env is generated at the time that the docker image bitnami/laravel was built, and the value of APP_KEY is fixed under certain conditions. This value is crucial for the security of the application and must be randomly generated per Laravel installation. If your application's encryption key is in the hands of a malicious party, that party could craft cookie values using the encryption key and exploit vulnerabilities inherent to PHP object serialization / unserialization, such as calling arbitrary class methods within your application.	7.3	More Details
CVE-2021-26962	A remote authenticated arbitrary command execution vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Vulnerabilities in the AirWave CLI could allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to full system compromise.	7.2	More Details
CVE-2021-26963	A remote authenticated arbitrary command execution vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Vulnerabilities in the AirWave CLI could allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to full system compromise.	7.2	More Details
CVE-2021-25346	A possible arbitrary memory overwrite vulnerabilities in quram library version prior to SMR Jan-2021 Release 1 allow arbitrary code execution.	7.1	More Details
CVE-2021-27364	An issue was discovered in the Linux kernel through 5.11.3. drivers/scsi/scsi_transport_iscsi.c is adversely affected by the ability of an unprivileged user to craft Netlink messages.	7.1	More Details
CVE-2021-26964	A remote authentication restriction bypass vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the AirWave web-based management interface could allow an authenticated remote attacker to improperly access and modify devices and management user details. A successful exploit would consist of an attacker using a lower privileged account to change management user or device details. This could allow the attacker to escalate privileges and/or change network details that they should not have access to.	7.1	More Details
CVE-2021-28041	ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.	7.1	More Details
CVE-2021-22128	An improper access control vulnerability in FortiProxy SSL VPN portal 2.0.0, 1.2.9 and below versions may allow an authenticated, remote attacker to access internal service such as the ZebOS Shell on the FortiProxy appliance through the Quick Connection functionality.	7.1	More Details
CVE-2021-25313	A Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rancher allows remote attackers to execute JavaScript via malicious links. This issue affects: SUSE Rancher Rancher versions prior to 2.5.6.	7.1	More Details
CVE-2021-21353	Pug is an npm package which is a high-performance template engine. In pug before version 3.0.1, if a remote attacker was able to control the `pretty` option of the pug compiler, e.g. if you spread a user provided object such as the query parameters of a request into the pug template inputs, it was possible for them to achieve remote code execution on the node.js backend. This is fixed in version 3.0.1. This advisory applies to multiple pug packages including "pug", "pug-code-gen". pug-code-gen has a backported fix at version 2.0.3. This advisory is not exploitable if there is no way for un-trusted input to be passed to pug as the `pretty` option, e.g. if you compile templates in advance before applying user input to them, you do not need to upgrade.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21324	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. In GLPI before version 9.5.4 there is an Insecure Direct Object Reference (IDOR) on "Solutions". This vulnerability gives an unauthorized user the ability to enumerate GLPI items names (including users logins) using the knowbase search form (requires authentication). To Reproduce: Perform a valid authentication at your GLPI instance, Browse the ticket list and select any open ticket, click on Solution form, then Search a solution form that will redirect you to the endpoint /"glpi/front/knowbaseitem.php?item_itemtype=Ticket&item_items_id=18&forcetab=Knowbase$1", and the item_itemtype=Ticket parameter present in the previous URL will point to the PHP alias of glpi_tickets table, so just replace it with "Users" to point to glpi_users table instead; in the same way, item_items_id=18 will point to the related column id, so changing it too you should be able to enumerate all the content which has an alias. Since such id(s) are obviously incremental, a malicious party could exploit the vulnerability simply by guessing-based attempts.	6.8	More Details
CVE-2021-21327	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. In GLPI before version 9.5.4 non-authenticated user can remotely instantiate object of any class existing in the GLPI environment that can be used to carry out malicious attacks, or to start a “POP chain”. As an example of direct impact, this vulnerability affects integrity of the GLPI core platform and third-party plugins runtime misusing classes which implement some sensitive operations in their constructors or destructors. This is fixed in version 9.5.4.	6.8	More Details
CVE-2021-27099	In SPIRE before versions 0.8.5, 0.9.4, 0.10.2, 0.11.3 and 0.12.1, the "aws_iid" Node Attestor improperly normalizes the path provided through the agent ID templating feature, which may allow the issuance of an arbitrary SPIFFE ID within the same trust domain, if the attacker controls the value of an EC2 tag prior to attestation, and the attestor is configured for agent ID templating where the tag value is the last element in the path. This issue has been fixed in SPIRE versions 0.11.3 and 0.12.1	6.8	More Details
CVE-2021-20262	A flaw was found in Keycloak 12.0.0 where re-authentication does not occur while updating the password. This flaw allows an attacker to take over an account if they can obtain temporary, physical access to a user’s browser. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	6.8	More Details
CVE-2021-21352	Anuko Time Tracker is an open source, web-based time tracking application written in PHP. In TimeTracker before version 1.19.24.5415 tokens used in password reset feature in Time Tracker are based on system time and, therefore, are predictable. This opens a window for brute force attacks to guess user tokens and, once successful, change user passwords, including that of a system administrator. This vulnerability is pathced in version 1.19.24.5415 (started to use more secure tokens) with an additional improvement in 1.19.24.5416 (limited an available window for brute force token guessing).	6.8	More Details
CVE-2021-3411	A flaw was found in the Linux kernel in versions prior to 5.10. A violation of memory access was found while detecting a padding of int3 in the linking state. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	6.7	More Details
CVE-2021-20225	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	6.7	More Details
CVE-2021-20253	A flaw was found in ansible-tower. The default installation is vulnerable to Job Isolation escape allowing an attacker to elevate the privilege from a low privileged user to the awx user from outside the isolated environment. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	6.7	More Details
CVE-2020-8296	Nextcloud Server prior to 20.0.0 stores passwords in a recoverable format even when external storage is not configured.	6.7	More Details
CVE-2020-27749	A flaw was found in grub2 in versions prior to 2.06. Variable names present are expanded in the supplied command line into their corresponding variable contents, using a 1kB stack buffer for temporary storage, without sufficient bounds checking. If the function is called with a command line that references a variable with a sufficiently large payload, it is possible to overflow the stack buffer, corrupt the stack frame and control execution which could also circumvent Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	6.7	More Details
CVE-2020-5014	IBM DataPower Gateway V10 and V2018 could allow a local attacker with administrative privileges to execute arbitrary code on the system using a server-side requesr forgery attack. IBM X-Force ID: 193247.	6.7	More Details
CVE-2021-26854	Microsoft Exchange Server Remote Code Execution Vulnerability	6.6	More Details
CVE-2021-26965	A remote authenticated sql injection vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Multiple vulnerabilities in the API of AirWave could allow an authenticated remote attacker to conduct SQL injection attacks against the AirWave instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database.	6.5	More Details
CVE-2021-26966	A remote authenticated sql injection vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Multiple vulnerabilities in the API of AirWave could allow an authenticated remote attacker to conduct SQL injection attacks against the AirWave instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22877	A missing user check in Nextcloud prior to 20.0.6 inadvertently populates a user's own credentials for other users external storage configuration when not already configured yet.	6.5	More Details
CVE-2021-21182	Insufficient policy enforcement in navigations in Google Chrome prior to 89.0.4389.72 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.	6.5	More Details
CVE-2021-21181	Side-channel information leakage in autofill in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	6.5	More Details
CVE-2021-21178	Inappropriate implementation in Compositing in Google Chrome on Linux and Windows prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	6.5	More Details
CVE-2020-28591	An out-of-bounds read vulnerability exists in the AMF File AMFParserContext::endElement() functionality of Slic3r libslic3r 1.3.0 and Master Commit 92abbc42. A specially crafted AMF file can lead to information disclosure. An attacker can provide a malicious file to trigger this vulnerability.	6.5	More Details
CVE-2021-21177	Insufficient policy enforcement in Autofill in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	6.5	More Details
CVE-2021-21176	Inappropriate implementation in full screen mode in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	6.5	More Details
CVE-2021-21175	Inappropriate implementation in Site isolation in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2020-35327	SQL injection vulnerability was discovered in Courier Management System 1.0, which can be exploited via the ref_no (POST) parameter to admin_class.php	6.5	More Details
CVE-2020-35329	Courier Management System 1.0 1.0 is affected by SQL Injection via 'MULTIPART street '.	6.5	More Details
CVE-2021-21173	Side-channel information leakage in Network Internals in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2021-21171	Incorrect security UI in TabStrip and Navigation in Google Chrome on Android prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	6.5	More Details
CVE-2021-27257	This vulnerability allows network-adjacent attackers to compromise the integrity of downloaded information on affected installations of NETGEAR R7800 firmware version 1.0.2.76. Authentication is not required to exploit this vulnerability. The specific flaw exists within the downloading of files via FTP. The issue results from the lack of proper validation of the certificate presented by the server. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-12362.	6.5	More Details
CVE-2021-21170	Incorrect security UI in Loader in Google Chrome prior to 89.0.4389.72 allowed a remote attacker who had compromised the renderer process to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	6.5	More Details
CVE-2021-21168	Insufficient policy enforcement in appcache in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	6.5	More Details
CVE-2021-22861	An improper access control vulnerability was identified in GitHub Enterprise Server that allowed authenticated users of the instance to gain write access to unauthorized repositories via specifically crafted pull requests and REST API requests. An attacker would need to be able to fork the targeted repository, a setting that is disabled by default for organization owned private repositories. Branch protections such as required pull request reviews or status checks would prevent unauthorized commits from being merged without further review or validation. This vulnerability affected all versions of GitHub Enterprise Server since 2.4.21 and was fixed in versions 2.20.24, 2.21.15, 2.22.7 and 3.0.1. This vulnerability was reported via the GitHub Bug Bounty program.	6.5	More Details
CVE-2021-21164	Insufficient data validation in Chrome on iOS in Google Chrome on iOS prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28039	An issue was discovered in the Linux kernel 5.9.x through 5.11.3, as used with Xen. In some less-common configurations, an x86 PV guest OS user can crash a Dom0 or driver domain via a large amount of I/O activity. The issue relates to misuse of guest physical addresses when a configuration has CONFIG_XEN_UNPOPULATED_ALLOC but not CONFIG_XEN_BALLOON_MEMORY_HOTPLUG.	6.5	More Details
CVE-2021-28038	An issue was discovered in the Linux kernel through 5.11.3, as used with Xen PV. A certain part of the netback driver lacks necessary treatment of errors such as failed memory allocations (as a result of changes to the handling of grant mapping errors). A host OS denial of service may occur during misbehavior of a networking frontend driver. NOTE: this issue exists because of an incomplete fix for CVE-2021-26931.	6.5	More Details
CVE-2021-21163	Insufficient data validation in Reader Mode in Google Chrome on iOS prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page and a malicious server.	6.5	More Details
CVE-2021-22862	An improper access control vulnerability was identified in GitHub Enterprise Server that allowed an authenticated user with the ability to fork a repository to disclose Actions secrets for the parent repository of the fork. This vulnerability existed due to a flaw that allowed the base reference of a pull request to be updated to point to an arbitrary SHA or another pull request outside of the fork repository. By establishing this incorrect reference in a PR, the restrictions that limit the Actions secrets sent a workflow from forks could be bypassed. This vulnerability affected GitHub Enterprise Server version 3.0.0, 3.0.0.rc2, and 3.0.0.rc1. This vulnerability was reported via the GitHub Bug Bounty program.	6.5	More Details
CVE-2021-21488	Knowledge Management versions 7.01, 7.02, 7.30, 7.31, 7.40, 7.50 allows a remote attacker with basic privileges to deserialize user-controlled data without verification, leading to insecure deserialization which triggers the attacker's code, therefore impacting Availability.	6.5	More Details
CVE-2021-26989	Clustered Data ONTAP versions prior to 9.3P21, 9.5P16, 9.6P12, 9.7P9 and 9.8 are susceptible to a vulnerability which could allow a remote authenticated attacker to cause a Denial of Service (DoS) on clustered Data ONTAP configured for SMB access.	6.5	More Details
CVE-2020-27838	A flaw was found in keycloak in versions prior to 13.0.0. The client registration endpoint allows fetching information about PUBLIC clients (like client secret) without authentication which could be an issue if the same PUBLIC client changed to CONFIDENTIAL later. The highest threat from this vulnerability is to data confidentiality.	6.5	More Details
CVE-2021-26969	A remote authenticated authenticated xml external entity (xxe) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Due to improper restrictions on XML entities a vulnerability exists in the web-based management interface of AirWave. A successful exploit could allow an authenticated attacker to retrieve files from the local system or cause the application to consume system resources, resulting in a denial of service condition.	6.5	More Details
CVE-2021-21336	Products.PluggableAuthService is a pluggable Zope authentication and authorization framework. In Products.PluggableAuthService before version 2.6.0 there is an information disclosure vulnerability - everyone can list the names of roles defined in the ZODB Role Manager plugin if the site uses this plugin. The problem has been fixed in version 2.6.0. Depending on how you have installed Products.PluggableAuthService, you should change the buildout version pin to 2.6.0 and re-run the buildout, or if you used pip simply do `pip install "Products.PluggableAuthService>=2.6.0"`.	6.5	More Details
CVE-2020-4903	IBM API Connect V10 and V2018 could allow an attacker who has intercepted a registration invitation link to impersonate the registered user or obtain sensitive information. IBM X-Force ID: 191105.	6.5	More Details
CVE-2021-21369	Hyperledger Besu is an open-source, MainNet compatible, Ethereum client written in Java. In Besu before version 1.5.1 there is a denial-of-service vulnerability involving the HTTP JSON-RPC API service. If username and password authentication is enabled for the HTTP JSON-RPC API service, then prior to making any requests to an API endpoint the requestor must use the login endpoint to obtain a JSON web token (JWT) using their credentials. A single user can readily overload the login endpoint with invalid requests (incorrect password). As the supplied password is checked for validity on the main vertx event loop and takes a relatively long time this can cause the processing of other valid requests to fail. A valid username is required for this vulnerability to be exposed. This has been fixed in version 1.5.1.	6.5	More Details
CVE-2021-26970	A remote authenticated arbitrary command execution vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Vulnerabilities in the AirWave web-base management interface could allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as a lower privileged user on the underlying operating system leading to partial system compromise.	6.3	More Details
CVE-2020-29028	Cross-site Scripting (XSS) vulnerability in web GUI of Secomea GateManager allows an attacker to inject arbitrary javascript code. This issue affects: Secomea GateManager all versions prior to 9.4.	6.3	More Details
CVE-2021-26971	A remote authenticated arbitrary command execution vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. Vulnerabilities in the AirWave web-base management interface could allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as a lower privileged user on the underlying operating system leading to partial system compromise.	6.3	More Details
CVE-2021-21325	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. In GLPI before version 9.5.4 a new budget type can be defined by user. This input is not correctly filtered. This results in a cross-site scripting attack. To exploit this endpoint attacker need to be authenticated. This is fixed in version 9.5.4.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25344	Missing permission check in knox_custom service prior to SMR Mar-2021 Release 1 allows attackers to gain access to device's serial number without permission.	6.2	More Details
CVE-2021-20663	Cross-site scripting vulnerability in in Role authority setting screen of Movable Type 7 r.4705 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.4705 and earlier (Movable Type Advanced 7 Series), Movable Type 6.7.5 and earlier (Movable Type 6.7 Series), Movable Type Premium 1.39 and earlier, and Movable Type Premium Advanced 1.39 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-23130	An issue was discovered in Joomla! 2.5.0 through 3.9.24. Missing filtering of feed fields could lead to xss issues.	6.1	More Details
CVE-2020-28150	I-Net Software Clear Reports 20.10.136 web application accepts a user-controlled input that specifies a link to an external site, and uses the user supplied data in a Redirect.	6.1	More Details
CVE-2021-28006	Web Based Quiz System 1.0 is affected by cross-site scripting (XSS) in admin.php through the options parameter.	6.1	More Details
CVE-2021-21510	Dell iDRAC8 versions prior to 2.75.100.75 contain a host header injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by injecting arbitrary ‘Host’ header values to poison a web-cache or trigger redirections.	6.1	More Details
CVE-2021-20664	Cross-site scripting vulnerability in in Asset registration screen of Movable Type 7 r.4705 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.4705 and earlier (Movable Type Advanced 7 Series), Movable Type 6.7.5 and earlier (Movable Type 6.7 Series), Movable Type Premium 1.39 and earlier, and Movable Type Premium Advanced 1.39 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-20665	Cross-site scripting vulnerability in in Add asset screen of Contents field of Movable Type 7 r.4705 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.4705 and earlier (Movable Type Advanced 7 Series), Movable Type Premium 1.39 and earlier, and Movable Type Premium Advanced 1.39 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-26967	A remote reflected cross-site scripting (xss) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the web-based management interface of AirWave could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of certain components of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim’s browser in the context of the AirWave management interface.	6.1	More Details
CVE-2020-35594	Zoho ManageEngine ADManager Plus before 7066 allows XSS.	6.1	More Details
CVE-2021-27940	resources/public/js/orchestrator.js in openark orchestrator before 3.2.4 allows XSS via the orchestrator-msg parameter.	6.1	More Details
CVE-2021-23129	An issue was discovered in Joomla! 2.5.0 through 3.9.24. Missing filtering of messages showed to users that could lead to xss issues.	6.1	More Details
CVE-2021-3377	The npm package ansi_up converts ANSI escape codes into HTML. In ansi_up v4, ANSI escape codes can be used to create HTML hyperlinks. Due to insufficient URL sanitization, this feature is affected by a cross-site scripting (XSS) vulnerability. This issue is fixed in v5.0.0.	6.1	More Details
CVE-2021-28115	The OUGC Feedback plugin before 1.8.23 for MyBB allows XSS via the comment field of feedback during an edit operation.	6.1	More Details
CVE-2020-24912	A reflected cross-site scripting (XSS) vulnerability in qcubed (all versions including 3.1.1) in profile.php via the stQuery-parameter allows unauthenticated attackers to steal sessions of authenticated users.	6.1	More Details
CVE-2021-23353	This affects the package jspdf before 2.3.1. ReDoS is possible via the addImage function.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21295	Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In Netty (io.netty:netty-codec-http2) before version 4.1.60.Final there is a vulnerability that enables request smuggling. If a Content-Length header is present in the original HTTP/2 request, the field is not validated by `Http2MultiplexHandler` as it is propagated up. This is fine as long as the request is not proxied through as HTTP/1.1. If the request comes in as an HTTP/2 stream, gets converted into the HTTP/1.1 domain objects (`HttpRequest`, `HttpContent`, etc.) via `Http2StreamFrameToHttpObjectCodec `and then sent up to the child channel's pipeline and proxied through a remote peer as HTTP/1.1 this may result in request smuggling. In a proxy case, users may assume the content-length is validated somehow, which is not the case. If the request is forwarded to a backend channel that is a HTTP/1.1 connection, the Content-Length now has meaning and needs to be checked. An attacker can smuggle requests inside the body as it gets downgraded from HTTP/2 to HTTP/1.1. For an example attack refer to the linked GitHub Advisory. Users are only affected if all of this is true: `HTTP2MultiplexCodec` or `Http2FrameCodec` is used, `Http2StreamFrameToHttpObjectCodec` is used to convert to HTTP/1.1 objects, and these HTTP/1.1 objects are forwarded to another remote peer. This has been patched in 4.1.60.Final As a workaround, the user can do the validation by themselves by implementing a custom `ChannelInboundHandler` that is put in the `ChannelPipeline` behind `Http2StreamFrameToHttpObjectCodec`.	5.9	More Details
CVE-2021-22189	Starting with version 13.7 the Gitlab CE/EE editions were affected by a security issue related to the validation of the certificates for the Fortinet OTP that could result in authentication issues.	5.9	More Details
CVE-2021-20441	IBM Security Verify Bridge uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 196617.	5.9	More Details
CVE-2021-21337	Products.PluggableAuthService is a pluggable Zope authentication and authorization framework. In Products.PluggableAuthService before version 2.6.0 there is an open redirect vulnerability. A maliciously crafted link to the login form and login functionality could redirect the browser to a different website. The problem has been fixed in version 2.6.1. Depending on how you have installed Products.PluggableAuthService, you should change the buildout version pin to `2.6.1` and re-run the buildout, or if you used `pip` simply do `pip install "Products.PluggableAuthService>=2.6.1".`	5.7	More Details
CVE-2021-21725	A ZTE product has an information leak vulnerability. An attacker with higher authority can go beyond their authority to access files in other directories by performing specific operations, resulting in information leak. This affects: ZXHN H196Q V9.1.0C2.	5.7	More Details
CVE-2021-24033	react-dev-utils prior to v11.0.4 exposes a function, getProcessForPort, where an input argument is concatenated into a command string to be executed. This function is typically used from react-scripts (in Create React App projects), where the usage is safe. Only when this function is manually invoked with user-provided values (ie: by custom code) is there the potential for command injection. If you're consuming it from react-scripts then this issue does not affect you.	5.6	More Details
CVE-2021-24031	In the Zstandard command-line utility prior to v1.4.1, output files were created with default permissions. Correct file permissions (matching the input) would only be set at completion time. Output files could therefore be readable or writable to unintended parties.	5.5	More Details
CVE-2021-20241	A flaw was found in ImageMagick in coders/jp2.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2020-8357	A denial of service vulnerability was reported in Lenovo PCManager, prior to version 3.0.200.2042, that could allow configuration files to be written to non-standard locations.	5.5	More Details
CVE-2021-26028	An issue was discovered in Joomla! 3.0.0 through 3.9.24. Extracting an specifilcy crafted zip package could write files outside of the intended path.	5.5	More Details
CVE-2021-25334	Improper input check in wallpaper service in Samsung mobile devices prior to SMR Feb-2021 Release 1 allows untrusted application to cause permanent denial of service.	5.5	More Details
CVE-2021-20244	A flaw was found in ImageMagick in MagickCore/visual-effects.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2021-20245	A flaw was found in ImageMagick in coders/webp.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2021-20246	A flaw was found in ImageMagick in MagickCore/resample.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. The highest threat from this vulnerability is to system availability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20243	A flaw was found in ImageMagick in MagickCore/resize.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2020-35521	A flaw was found in libtiff. Due to a memory allocation failure in tif_read.c, a crafted TIFF file can lead to an abort, resulting in denial of service.	5.5	More Details
CVE-2020-35522	In LibTIFF, there is a memory malloc failure in tif_pixarlog.c. A crafted TIFF document can lead to an abort, resulting in a remote denial of service attack.	5.5	More Details
CVE-2021-25252	Trend Micro's Virus Scan API (VSAPI) and Advanced Threat Scan Engine (ATSE) - are vulnerable to a memory exhaustion vulnerability that may lead to denial-of-service or system freeze if exploited by an attacker using a specially crafted file.	5.5	More Details
CVE-2021-20255	A stack overflow via an infinite recursion vulnerability was found in the eepro100 i8255x device emulator of QEMU. This issue occurs while processing controller commands due to a DMA reentry issue. This flaw allows a guest user or process to consume CPU cycles or crash the QEMU process on the host, resulting in a denial of service. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2020-4863	IBM Engineering products are 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: 190566.	5.4	More Details
CVE-2020-4866	IBM Engineering products are 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: 190742.	5.4	More Details
CVE-2021-27907	Apache Superset up to and including 0.38.0 allowed the creation of a Markdown component on a Dashboard page for describing chart's related information. Abusing this functionality, a malicious user could inject javascript code executing unwanted action in the context of the user's browser. The javascript code will be automatically executed (Stored XSS) when a legitimate user surfs on the dashboard page. The vulnerability is exploitable creating a “div” section and embedding in it a “svg” element with javascript code.	5.4	More Details
CVE-2021-20340	IBM Engineering products are 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: 194451.	5.4	More Details
CVE-2021-21314	GLPI is open source software which stands for Gestionnaire Libre de Parc Informatique and it is a Free Asset and IT Management Software package. In GLPI before verison 9.5.4, there is an XSS vulnerability involving a logged in user while updating a ticket.	5.4	More Details
CVE-2020-4975	IBM Engineering products are 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: 192435.	5.4	More Details
CVE-2021-21312	GLPI is open source software which stands for Gestionnaire Libre de Parc Informatique and it is a Free Asset and IT Management Software package. In GLPI before verison 9.5.4, there is a vulnerability within the document upload function (Home > Management > Documents > Add, or /front/document.form.php endpoint), indeed one of the form field: "Web Link" is not properly sanitized and a malicious user (who has document upload rights) can use it to deliver JavaScript payload. For example if you use the following payload: " accesskey="x" onclick="alert(1)" x=", the content will be saved within the database without any control. And then once you return to the summary documents page, by clicking on the "Web Link" of the newly created file it will create a new empty tab, but on the initial tab the pop-up "1" will appear.	5.4	More Details
CVE-2021-27222	In the "Time in Status" app before 4.13.0 for Jira, remote authenticated attackers can cause Stored XSS.	5.4	More Details
CVE-2020-27576	Maxum Rumpus 8.2.13 and 8.2.14 is affected by cross-site scripting (XSS). Users are able to create folders in the web application. The folder name is insufficiently validated resulting in a stored cross-site scripting vulnerability.	5.4	More Details
CVE-2021-20351	IBM Engineering products are 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: 194708.	5.4	More Details
CVE-2020-4857	IBM Engineering products are 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: 190460.	5.4	More Details
CVE-2020-4856	IBM Engineering products are 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: 190459.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35328	Courier Management System 1.0 - 'First Name' Stored XSS	5.4	More Details
CVE-2021-20350	IBM Engineering products are 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: 194707.	5.4	More Details
CVE-2021-20341	IBM Cloud Pak for Multicloud Management Monitoring 2.2 returns potentially sensitive information in headers which could lead to further attacks against the system. IBM X-Force ID: 194513.	5.3	More Details
CVE-2019-25025	The activerecord-session_store (aka Active Record Session Store) component through 1.1.3 for Ruby on Rails does not use a constant-time approach when delivering information about whether a guessed session ID is valid. Consequently, remote attackers can leverage timing discrepancies to achieve a correct guess in a relatively short amount of time. This is a related issue to CVE-2019-16782.	5.3	More Details
CVE-2021-21335	In the SPNEGO HTTP Authentication Module for nginx (spnego-http-auth-nginx-module) before version 1.1.1 basic Authentication can be bypassed using a malformed username. This affects users of spnego-http-auth-nginx-module that have enabled basic authentication. This is fixed in version 1.1.1 of spnego-http-auth-nginx-module. As a workaround, one may disable basic authentication.	5.3	More Details
CVE-2021-26027	An issue was discovered in Joomla! 3.0.0 through 3.9.24. Incorrect ACL checks could allow unauthorized change of the category for an article.	5.3	More Details
CVE-2021-25347	Hijacking vulnerability in Samsung Email application version prior to SMR Feb-2021 Release 1 allows attackers to intercept when the provider is executed.	5.3	More Details
CVE-2021-26029	An issue was discovered in Joomla! 1.6.0 through 3.9.24. Inadequate filtering of form contents could allow to overwrite the author field.	5.3	More Details
CVE-2021-21360	Products.GenericSetup is a mini-framework for expressing the configured state of a Zope Site as a set of filesystem artifacts. In Products.GenericSetup before version 2.1.1 there is an information disclosure vulnerability - anonymous visitors may view log and snapshot files generated by the Generic Setup Tool. The problem has been fixed in version 2.1.1. Depending on how you have installed Products.GenericSetup, you should change the buildout version pin to 2.1.1 and re-run the buildout, or if you used pip simply do pip install `"Products.GenericSetup>=2.1.1"`.	5.3	More Details
CVE-2021-23126	An issue was discovered in Joomla! 3.2.0 through 3.9.24. Usage of the insecure rand() function within the process of generating the 2FA secret.	5.3	More Details
CVE-2021-22188	An issue has been discovered in GitLab affecting all versions starting with 13.0. Confidential issue titles in Gitlab were readable by an unauthorised user via branch logs.	5.3	More Details
CVE-2021-21361	The `com.bmuschko:gradle-vagrant-plugin` Gradle plugin contains an information disclosure vulnerability due to the logging of the system environment variables. When this Gradle plugin is executed in public CI/CD, this can lead to sensitive credentials being exposed to malicious actors. This is fixed in version 3.0.0.	5.3	More Details
CVE-2021-25340	Improper access control vulnerability in Samsung keyboard version prior to SMR Feb-2021 Release 1 allows physically proximate attackers to change in arbitrary settings during Initialization State.	5.1	More Details
CVE-2021-3417	An internal product security audit of LXCO, prior to version 1.2.2, discovered that credentials for Lenovo XClarity Administrator (LXCA), if added as a Resource Manager, are encoded then written to an internal LXCO log file each time a session is established with LXCA. Affected logs are captured in the First Failure Data Capture (FFDC) service log. The FFDC service log is only generated when requested by a privileged LXCO user and it is only accessible to the privileged LXCO user that requested the file.	4.9	More Details
CVE-2019-18628	Xerox AltaLink B8045/B8055/B8065/B8075/B8090 and C8030/C8035/C8045/C8055/C8070 multifunction printers with software releases before 101.00x.099.28200 allow a user with administrative privileges to turn off data encryption on the device, thus leaving it open to potential cryptographic information disclosure.	4.9	More Details
CVE-2021-21313	GLPI is open source software which stands for Gestionnaire Libre de Parc Informatique and it is a Free Asset and IT Management Software package. In GLPI before verison 9.5.4, there is a vulnerability in the /ajax/common.tabs.php endpoint, indeed, at least two parameters _target and id are not properly sanitized. Here are two payloads (due to two different exploitations depending on which parameter you act) to exploit the vulnerability:/ajax/common.tabs.php?_target=javascript:alert(document.cookie)&_itemtype=DisplayPreference&_glpi_tab=DisplayPreference$2&id=258&displaytype=Ticket (Payload triggered if you click on the button). /ajax/common.tabs.php?_target=/front/ticket.form.php&_itemtype=Ticket&_glpi_tab=Ticket$1&id=(){};(function%20(){alert(document.cookie);})();function%20a&#.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8356	An internal product security audit of LXCO, prior to version 1.2.2, discovered that optional passwords, if specified, for the Syslog and SMTP forwarders are written to an internal LXCO log file in clear text. Affected logs are captured in the First Failure Data Capture (FFDC) service log. The FFDC service log is only generated when requested by a privileged LXCO user and it is only accessible to the privileged LXCO user that requested the file.	4.9	More Details
CVE-2021-26968	A remote authenticated stored cross-site scripting (xss) vulnerability was discovered in Aruba AirWave Management Platform version(s): Prior to 8.2.12.0. A vulnerability in the web-based management interface of AirWave could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	4.8	More Details
CVE-2021-23346	This affects the package html-parse-stringify before 2.0.1; all versions of package html-parse-stringify2. Sending certain input could cause one of the regular expressions that is used for parsing to backtrack, freezing the process.	4.8	More Details
CVE-2021-22878	Nextcloud Server prior to 20.0.6 is vulnerable to reflected cross-site scripting (XSS) due to lack of sanitization in `OC.Notification.show`.	4.8	More Details
CVE-2020-15937	An improper neutralization of input vulnerability in FortiGate version 6.2.x below 6.2.5 and 6.4.x below 6.4.1 may allow a remote attacker to perform a stored cross site scripting attack (XSS) via the IPS and WAF logs dashboard.	4.7	More Details
CVE-2020-35451	There is a race condition in OozieSharelibCLI in Apache Oozie before version 5.2.1 which allows a malicious attacker to replace the files in Oozie's sharelib during it's creation.	4.7	More Details
CVE-2021-24032	Beginning in v1.4.1 and prior to v1.4.9, due to an incomplete fix for CVE-2021-24031, the Zstandard command-line utility created output files with default permissions and restricted those permissions immediately afterwards. Output files could therefore momentarily be readable or writable to unintended parties.	4.7	More Details
CVE-2021-23347	The package github.com/argoproj/argo-cd/cmd before 1.7.13, from 1.8.0 and before 1.8.6 are vulnerable to Cross-site Scripting (XSS) the SSO provider connected to Argo CD would have to send back a malicious error message containing JavaScript to the user.	4.7	More Details
CVE-2021-2138	Vulnerability in the Oracle Cloud Infrastructure Data Science Notebook Sessions. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the Oracle Cloud Infrastructure Data Science Notebook Sessions executes to compromise Oracle Cloud Infrastructure Data Science Notebook Sessions. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Cloud Infrastructure Data Science Notebook Sessions accessible data as well as unauthorized read access to a subset of Oracle Cloud Infrastructure Data Science Notebook Sessions accessible data. All affected customers were notified of CVE-2021-2138 by Oracle. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N)	4.6	More Details
CVE-2021-27839	A CSV injection vulnerability found in Online Invoicing System (OIS) 4.3 and below can be exploited by users to perform malicious actions such as redirecting admins to unknown or harmful websites, or disclosing other clients' details that the user did not have access to.	4.4	More Details
CVE-2021-23351	The package github.com/pires/go-proxyproto before 0.5.0 are vulnerable to Denial of Service (DoS) via the parseVersion1() function. The reader in this package is a default bufio.Reader wrapping a net.Conn. It will read from the connection until it finds a newline. Since no limits are implemented in the code, a deliberately malformed V1 header could be used to exhaust memory in a server process using this code - and create a DoS. This can be exploited by sending a stream starting with PROXY and continuing to send data (which does not contain a newline) until the target stops acknowledging. The risk here is small, because only trusted sources should be allowed to send proxy protocol headers.	4.4	More Details
CVE-2021-25337	Improper access control in clipboard service in Samsung mobile devices prior to SMR Mar-2021 Release 1 allows untrusted applications to read or write certain local files.	4.4	More Details
CVE-2021-27217	An issue was discovered in the _send_secure_msg() function of Yubico yubihsm-shell through 2.0.3. The function does not correctly validate the embedded length field of an authenticated message received from the device. Out-of-bounds reads performed by aes_remove_padding() can crash the running process, depending on the memory layout. This could be used by an attacker to cause a client-side denial of service. The yubihsm-shell project is included in the YubiHSM 2 SDK product.	4.4	More Details
CVE-2021-25339	Improper address validation in HArx in Samsung mobile devices prior to SMR Mar-2021 Release 1 allows an attacker, given a compromised kernel, to corrupt EL2 memory.	4.4	More Details
CVE-2020-25639	A NULL pointer dereference flaw was found in the Linux kernel's GPU Nouveau driver functionality in versions prior to 5.12-rc1 in the way the user calls ioctl DRM_IOCTL_NOUVEAU_CHANNEL_ALLOC. This flaw allows a local user to crash the system.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27363	An issue was discovered in the Linux kernel through 5.11.3. A kernel pointer leak can be used to determine the address of the iscsi_transport structure. When an iSCSI transport is registered with the iSCSI subsystem, the transport's handle is available to unprivileged users via the sysfs file system, at /sys/class/iscsi_transport/$TRANSPORT_NAME/handle. When read, the show_transport_handle function (in drivers/scsi/scsi_transport_iscsi.c) is called, which leaks the handle. This handle is actually the pointer to an iscsi_transport struct in the kernel module's global variables.	4.4	More Details
CVE-2021-25338	Improper memory access control in RKP in Samsung mobile devices prior to SMR Mar-2021 Release 1 allows an attacker, given a compromised kernel, to write certain part of RKP EL2 memory region.	4.4	More Details
CVE-2021-21185	Insufficient policy enforcement in extensions in Google Chrome prior to 89.0.4389.72 allowed an attacker who convinced a user to install a malicious extension to obtain sensitive information via a crafted Chrome Extension.	4.3	More Details
CVE-2021-21189	Insufficient policy enforcement in payments in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	4.3	More Details
CVE-2021-21187	Insufficient data validation in URL formatting in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	4.3	More Details
CVE-2021-21186	Insufficient policy enforcement in QR scanning in Google Chrome on iOS prior to 89.0.4389.72 allowed an attacker who convinced the user to scan a QR code to bypass navigation restrictions via a crafted QR code.	4.3	More Details
CVE-2021-21184	Inappropriate implementation in performance APIs in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	4.3	More Details
CVE-2021-21183	Inappropriate implementation in performance APIs in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	4.3	More Details
CVE-2021-22134	A document disclosure flaw was found in Elasticsearch versions after 7.6.0 and before 7.11.0 when Document or Field Level Security is used. Get requests do not properly apply security permissions when executing a query against a recently updated document. This affects documents that have been updated and not yet refreshed in the index. This could result in the search disclosing the existence of documents and fields the attacker should not be able to view.	4.3	More Details
CVE-2021-22183	An issue has been discovered in GitLab affecting all versions starting with 11.8. GitLab was vulnerable to a stored XSS in the epics page, which could be exploited with user interactions.	4.1	More Details
CVE-2021-25342	Calling of non-existent provider in SMP sdk prior to version 3.0.9 allows unauthorized actions including denial of service attack by hijacking the provider.	4.0	More Details
CVE-2021-25341	Calling of non-existent provider in S Assistant prior to version 6.5.01.22 allows unauthorized actions including denial of service attack by hijacking the provider.	4.0	More Details
CVE-2021-25343	Calling of non-existent provider in Samsung Members prior to version 2.4.81.13 (in Android O(8.1) and below) and 3.8.00.13 (in Android P(9.0) and above) allows unauthorized actions including denial of service attack by hijacking the provider.	4.0	More Details
CVE-2021-25345	Graphic format mismatch while converting video format in hwcomposer prior to SMR Mar-2021 Release 1 results in kernel panic due to unsupported format.	4.0	More Details
CVE-2020-15938	When traffic other than HTTP/S (eg: SSH traffic, etc...) traverses the FortiGate in version below 6.2.5 and below 6.4.2 on port 80/443, it is not redirected to the transparent proxy policy for processing, as it doesn't have a valid HTTP header.	4.0	More Details
CVE-2021-28116	Squid through 4.14 and 5.x through 5.0.5, in some configurations, allows information disclosure because of an out-of-bounds read in WCCP protocol data. This can be leveraged as part of a chain for remote code execution as nobody.	3.7	More Details
CVE-2021-22182	An issue has been discovered in GitLab affecting all versions starting with 13.7. GitLab was vulnerable to a stored XSS in merge request.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26988	Clustered Data ONTAP versions prior to 9.3P21, 9.5P16, 9.6P12, 9.7P8 and 9.8 are susceptible to a vulnerability which could allow unauthorized tenant users to discover information related to converting a 7-Mode directory to Cluster-mode such as Storage Virtual Machine (SVM) names, volume names, directory paths and Job IDs.	3.5	More Details
CVE-2021-21493	When a user opens manipulated Graphics Interchange Format (.GIF) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	3.3	More Details
CVE-2021-27584	When a user opens manipulated PhotoShop Document (.PSD) format files received from untrusted sources in SAP 3D Visual Enterprise Viewer version 9, the application crashes and becomes temporarily unavailable to the user until restart of the application.	3.3	More Details
CVE-2021-20263	A flaw was found in the virtio-fs shared file system daemon (virtiofsd) of QEMU. The new 'xattrmap' option may cause the 'security.capability' xattr in the guest to not drop on file write, potentially leading to a modified, privileged executable in the guest. In rare circumstances, this flaw could be used by a malicious user to elevate their privileges within the guest.	3.3	More Details
CVE-2021-25333	Improper access control in Samsung Pay mini application prior to v4.0.14 allows unauthorized access to balance information over the lockscreen via scanning specific QR code.	3.2	More Details
CVE-2021-25332	Improper access control in Samsung Pay mini application prior to v4.0.14 allows unauthorized access to contacts information over the lockscreen in specific condition.	3.2	More Details
CVE-2021-25331	Improper access control in Samsung Pay mini application prior to v4.0.14 allows unauthorized access to balance information over the lockscreen in specific condition.	3.2	More Details
CVE-2021-21331	The Java client for the Datadog API before version 1.0.0-beta.9 has a local information disclosure of sensitive information downloaded via the API using the API Client. The Datadog API is executed on a unix-like system with multiple users. The API is used to download a file containing sensitive information. This sensitive information is exposed locally to other users. This vulnerability exists in the API Client for version 1 and 2. The method `prepareDownloadFilecreates` creates a temporary file with the permissions bits of `-rw-r--r--` on unix-like systems. On unix-like systems, the system temporary directory is shared between users. As such, the contents of the file downloaded via the `downloadFileFromResponse` method will be visible to all other users on the local system. Analysis of the finding determined that the affected code was unused, meaning that the exploitation likelihood is low. The unused code has been removed, effectively mitigating this issue. This issue has been patched in version 1.0.0-beta.9. As a workaround one may specify `java.io.tmpdir` when starting the JVM with the flag `-Djava.io.tmpdir`, specifying a path to a directory with `drw-------` permissions owned by `dd-agent`.	3.0	More Details
CVE-2021-25336	Improper access control in NotificationManagerService in Samsung mobile devices prior to SMR Mar-2021 Release 1 allows untrusted applications to acquire notification access via sending a crafted malicious intent.	2.8	More Details
CVE-2021-25335	Improper lockscreen status check in cocktailbar service in Samsung mobile devices prior to SMR Mar-2021 Release 1 allows unauthenticated users to access hidden notification contents over the lockscreen in specific condition.	2.5	More Details
CVE-2021-25348	Improper permission grant check in Samsung Internet prior to version 13.0.1.60 allows access to files in internal storage without authorized STORAGE permission.	2.1	More Details
CVE-2021-3419	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2019-18351	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-18790. Reason: This candidate is a duplicate of CVE-2019-18790. Notes: All CVE users should reference CVE-2019-18790 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-27817	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA	N/A	More Details