SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 25 November 2020

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-2020-6016	Valve's Game Networking Sockets prior to version v1.2.0 improperly handles unreliable segments with negative offsets in function SNP_ReceiveUnreliableSegment(), leading to a Heap-Based Buffer Underflow and a free() of memory not from the heap, resulting in a memory corruption and probably even a remote code execution.	9.8	More Details
CVE-2020-28334	Barco wePresent WiPG-1600W devices use Hard-coded Credentials (issue 2 of 2). Affected Version(s): 2.5.1.8, 2.5.0.25, 2.5.0.24, 2.4.1.19. The Barco wePresent WiPG-1600W device has a hardcoded root password hash included in the firmware image. Exploiting CVE-2020-28329, CVE-2020-28330 and CVE-2020-28331 could potentially be used in a simple and automated exploit chain to go from unauthenticated remote attacker to root shell.	9.8	More Details
CVE-2020-15929	In Ortus TestBox 2.4.0 through 4.1.0, unvalidated query string parameters passed to system/runners/HTMLRunner.cfm allow an attacker to write an arbitrary CFM file (within the application's context) containing attacker-defined CFML tags, leading to Remote Code Execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25475	SimplePHPscripts News Script PHP Pro 2.3 is affected by a SQL Injection via the id parameter in an editNews action.	9.8	More Details
CVE-2020-29006	MISP before 2.4.135 lacks an ACL check, related to app/Controller/GalaxyElementsController.php and app/Model/GalaxyElement.php.	9.8	More Details
CVE-2020-4001	The SD-WAN Orchestrator 3.3.2, 3.4.x, and 4.0.x has default passwords allowing for a Pass-the-Hash Attack. SD-WAN Orchestrator ships with default passwords for predefined accounts which may lead to to a Pass-the-Hash attack.	9.8	More Details
CVE-2020-13942	It is possible to inject malicious OGNL or MVEL scripts into the /context.json public endpoint. This was partially fixed in 1.5.1 but a new attack vector was found. In Apache Unomi version 1.5.2 scripts are now completely filtered from the input. It is highly recommended to upgrade to the latest available version of the 1.5.x release to fix this problem.	9.8	More Details
CVE-2020-28994	A SQL injection vulnerability was discovered in Karenderia Multiple Restaurant System, affecting versions 5.4.2 and below. The vulnerability allows for an unauthenticated attacker to perform various tasks such as modifying and leaking all contents of the database.	9.8	More Details
CVE-2020-28332	Barco wePresent WiPG-1600W devices download code without an Integrity Check. Affected Version(s): 2.5.1.8, 2.5.0.25, 2.5.0.24, 2.4.1.19. The Barco wePresent WiPG-1600W firmware does not perform verification of digitally signed firmware updates and is susceptible to processing and installing modified/malicious images.	9.8	More Details
CVE-2020-28333	Barco wePresent WiPG-1600W devices allow Authentication Bypass. Affected Version(s): 2.5.1.8. The Barco wePresent WiPG-1600W web interface does not use session cookies for tracking authenticated sessions. Instead, the web interface uses a "SEID" token that is appended to the end of URLs in GET requests. Thus the "SEID" would be exposed in web proxy logs and browser history. An attacker that is able to capture the "SEID" and originate requests from the same IP address (via a NAT device or web proxy) would be able to access the user interface of the device without having to know the credentials.	9.8	More Details
CVE-2020-25159	499ES EtherNet/IP (ENIP) Adaptor Source Code is vulnerable to a stack-based buffer overflow, which may allow an attacker to send a specially crafted packet that may result in a denial-of-service condition or code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26097	The firmware of the PLANET Technology Corp NVR-915 and NVR-1615 before 2020-10-28 embeds default credentials for root access via telnet. By exposing telnet on the Internet, remote root access on the device is possible. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.8	More Details
CVE-2020-28329	Barco wePresent WiPG-1600W firmware includes a hardcoded API account and password that is discoverable by inspecting the firmware image. A malicious actor could use this password to access authenticated, administrative functions in the API. Affected Version(s): 2.5.1.8, 2.5.0.25, 2.5.0.24, 2.4.1.19.	9.8	More Details
CVE-2015-9551	An issue was discovered on TOTOLINK A850R-V1 through 1.0.1-B20150707.1612 and F1-V2 through 1.1-B20150708.1646 devices. There is Remote Code Execution in the management interface via the formSysCmd sysCmd parameter.	9.8	More Details
CVE-2020-29054	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. Attackers can use "show system infor" to discover cleartext TELNET credentials.	9.8	More Details
CVE-2020-29056	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. One can escape from a shell and acquire root privileges by leveraging the TFTP download configuration.	9.8	More Details
CVE-2020-29058	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. Attackers can discover cleartext web-server credentials via certain /opt/lighttpd/web/cgi/ requests.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29059	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default panger123 password for the suma123 account for certain old firmware.	9.8	More Details
CVE-2020-29060	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default debug124 password for the debug account.	9.8	More Details
CVE-2020-29061	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default root126 password for the root account.	9.8	More Details
CVE-2020-28991	Gitea 0.9.99 through 1.12.x before 1.12.6 does not prevent a git protocol path that specifies a TCP port number and also contains newlines (with URL encoding) in ParseRemoteAddr in modules/auth/repo_form.go.	9.8	More Details
CVE-2020-29062	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default blank password for the guest account.	9.8	More Details
CVE-2020-28984	prive/formulaires/configurer_preferences.php in SPIP before 3.2.8 does not properly validate the couleur, display, display_navigation, display_outils, imessage, and spip_ecran parameters.	9.8	More Details
CVE-2020-28212	A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists in PLC Simulator on EcoStruxure[a] Control Expert (now Unity Pro) (all versions) that could cause unauthorized command execution when a brute force attack is done over Modbus.	9.8	More Details
CVE-2020-28578	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an unauthenticated, remote attacker to send a specially crafted HTTP message and achieve remote code execution with elevated privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3470	Multiple vulnerabilities in the API subsystem of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges. The vulnerabilities are due to improper boundary checks for certain user-supplied input. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the API subsystem of an affected system. When this request is processed, an exploitable buffer overflow condition may occur. A successful exploit could allow the attacker to execute arbitrary code with root privileges on the underlying operating system (OS).	9.8	More Details
CVE-2020-3531	A vulnerability in the REST API of Cisco IoT Field Network Director (FND) could allow an unauthenticated, remote attacker to access the back-end database of an affected system. The vulnerability exists because the affected software does not properly authenticate REST API calls. An attacker could exploit this vulnerability by obtaining a cross-site request forgery (CSRF) token and then using the token with REST API requests. A successful exploit could allow the attacker to access the back-end database of the affected device and read, alter, or drop information.	9.8	More Details
CVE-2019-20933	InfluxDB before 1.7.6 has an authentication bypass vulnerability in the authenticate function in services/httpd/handler.go because a JWT token may have an empty SharedSecret (aka shared secret).	9.8	More Details
CVE-2020-11829	Dynamic loading of services in the backup and restore SDK leads to elevated privileges, affected product is com.coloros.codebook V2.0.0_5493e40_200722.	9.8	More Details
CVE-2020-11830	QualityProtect has a vulnerability to execute arbitrary system commands, affected product is com.oppo.qualityprotect V2.0.	9.8	More Details
CVE-2020-11831	OvoiceManager has system permission to write vulnerability reports for arbitrary files, affected product is com.oppo.ovoicemanager V2.0.1.	9.8	More Details
CVE-2020-28360	Insufficient RegEx in private-ip npm package v1.0.5 and below insufficiently filters reserved IP ranges resulting in indeterminate SSRF. An attacker can perform a large range of requests to ARIN reserved IP ranges, resulting in an indeterminable number of critical attack vectors, allowing remote attackers to request server-side resources or potentially execute arbitrary code through various SSRF techniques.	9.8	More Details
CVE-2020-28951	libuci in OpenWrt before 18.06.9 and 19.x before 19.07.5 may encounter a use after free when using malicious package names. This is related to uci_parse_package in file.c and uci_strdup in util.c.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7561	A CWE-306: Missing Authentication for Critical Function vulnerability exists in Easergy T300 (with firmware 2.7 and older) that could cause a wide range of problems, including information exposure, denial of service, and command execution when access to a resource from an attacker is not restricted or incorrectly restricted.	9.8	More Details
CVE-2020-25839	NetIQ Identity Manager 4.8 prior to version 4.8 SP2 HF1 are affected by an injection vulnerability. This vulnerability is fixed in NetIQ IdM 4.8 SP2 HF1.	9.8	More Details
CVE-2020-28877	Buffer overflow in in the copy_msg_element function for the devDiscoverHandle server in the TP-Link WR and WDR series, including WDR7400, WDR7500, WDR7660, WDR7800, WDR8400, WDR8500, WDR8600, WDR8620, WDR8640, WDR8660, WR880N, WR886N, WR890N, WR890N, WR882N, and WR708N.	9.8	More Details
CVE-2020-25189	The affected product is vulnerable to three stack-based buffer overflows, which may allow an unauthenticated attacker to remotely execute arbitrary code on the IP150 (firmware versions 5.02.09).	9.8	More Details
CVE-2020-4854	IBM Spectrum Protect Plus 10.1.0 thorugh 10.1.6 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: 190454.	9.8	More Details
CVE-2020-6939	Tableau Server installations configured with Site-Specific SAML that allows the APIs to be used by unauthenticated users. If exploited, this could allow a malicious user to configure Site-Specific SAML settings and could lead to account takeover for users of that site. Tableau Server versions affected on both Windows and Linux are: 2018.2 through 2018.2.27, 2018.3 through 2018.3.24, 2019.1 through 2019.1.22, 2019.2 through 2019.2.18, 2019.3 through 2019.3.14, 2019.4 through 2019.4.13, 2020.1 through 2020.1.10, 2020.2 through 2020.2.7, and 2020.3 through 2020.3.2.	9.8	More Details
CVE-2020-28864	Buffer overflow in WinSCP 5.17.8 allows a malicious FTP server to cause a denial of service or possibly have other unspecified impact via a long file name.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3586	A vulnerability in the web-based management interface of Cisco DNA Spaces Connector could allow an unauthenticated, remote attacker to execute arbitrary commands on an affected device. The vulnerability is due to insufficient validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on the underling operating system with privileges of the web-based management application, which is running as a restricted user. This could result in changes being made to pages served by the web-based management application impacting the integrity or availability of the web-based management application.	9.4	More Details
CVE-2020-12495	Endress+Hauser Ecograph T (Neutral/Private Label) (RSG35, ORSG35) with Firmware version prior to V2.0.0 is prone to improper privilege management. The affected device has a web-based user interface with a role-based access system. Users with different roles have different write and read privileges. The access system is based on dynamic "tokens". The vulnerability is that user sessions are not closed correctly and a user with fewer rights is assigned the higher rights when he logs on.	9.1	More Details
CVE-2020-7378	CRIXP OpenCRX version 4.30 and 5.0-20200717 and prior suffers from an unverified password change vulnerability. An attacker who is able to connect to the affected OpenCRX instance can change the password of any user, including admin-Standard, to any chosen value. This issue was resolved in version 5.0-20200904, released September 4, 2020.	9.1	More Details
CVE-2020-4006	VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector address have a command injection vulnerability.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-7572	A CWE-611 Improper Restriction of XML External Entity Reference vulnerability exists in EcoStruxure Building Operation WebReports V1.9 - V3.1 that could cause an authenticated remote user being able to inject arbitrary XML code and obtain disclosure of confidential data, denial of service, server side request forgery due to improper configuration of the XML parser.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29040	An issue was discovered in Xen through 4.14.x allowing x86 HVM guest OS users to cause a denial of service (stack corruption), cause a data leak, or possibly gain privileges because of an off-by-one error. NOTE: this issue is caused by an incorrect fix for CVE-2020-27671.	8.8	More Details
CVE-2020-7569	A CWE-434 Unrestricted Upload of File with Dangerous Type vulnerability exists in EcoStruxure Building Operation WebReports V1.9 - V3.1 that could cause an authenticated remote user being able to upload arbitrary files due to incorrect verification of user supplied files and achieve remote code execution.	8.8	More Details
CVE-2020-25660	A flaw was found in the Cephx authentication protocol in versions before 15.2.6 and before 14.2.14, where it does not verify Ceph clients correctly and is then vulnerable to replay attacks in Nautilus. This flaw allows an attacker with access to the Ceph cluster network to authenticate with the Ceph service via a packet sniffer and perform actions allowed by the Ceph service. This issue is a reintroduction of CVE-2018-1128, affecting the msgr2 protocol. The msgr 2 protocol is used for all communication except older clients that do not support the msgr2 protocol. The msgr1 protocol is not affected. The highest threat from this vulnerability is to confidentiality, integrity, and system availability.	8.8	More Details
CVE-2020-13671	Drupal core does not properly sanitize certain filenames on uploaded files, which can lead to files being interpreted as the incorrect extension and served as the wrong MIME type or executed as PHP for certain hosting configurations. This issue affects: Drupal Drupal Core 9.0 versions prior to 9.0.8, 8.9 versions prior to 8.9.9, 8.8 versions prior to 8.8.11, and 7 versions prior to 7.74.	8.8	More Details
CVE-2020-26075	A vulnerability in the REST API of Cisco IoT Field Network Director (FND) could allow an authenticated, remote attacker to gain access to the back-end database of an affected device. The vulnerability is due to insufficient input validation of REST API requests that are made to an affected device. An attacker could exploit this vulnerability by crafting malicious API requests to the affected device. A successful exploit could allow the attacker to gain access to the back-end database of the affected device.	8.8	More Details
CVE-2020-25185	The affected product is vulnerable to five post-authentication buffer overflows, which may allow a logged in user to remotely execute arbitrary code on the IP150 (firmware versions 5.02.09).	8.8	More Details
CVE-2020-13620	Fastweb FASTGate GPON FGA2130FWB devices through 2020-05-26 allow CSRF via the router administration web panel, leading to an attacker's ability to perform administrative actions such as modifying the configuration.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3985	The SD-WAN Orchestrator 3.3.2 prior to 3.3.2 P3 and 3.4.x prior to 3.4.4 allows an access to set arbitrary authorization levels leading to a privilege escalation issue. An authenticated SD-WAN Orchestrator user may exploit an application weakness and call a vulnerable API to elevate their privileges.	8.8	More Details
CVE-2020-28213	A CWE-494: Download of Code Without Integrity Check vulnerability exists in PLC Simulator on EcoStruxure[a] Control Expert (now Unity Pro) (all versions) that could cause unauthorized command execution when sending specially crafted requests over Modbus.	8.8	More Details
CVE-2020-12351	Improper input validation in BlueZ may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2020-7564	A CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability exists in the Web Server on Modicon M340, Modicon Quantum and Modicon Premium Legacy offers and their Communication Modules (see notification for details) which could cause write access and the execution of commands when uploading a specially crafted file on the controller over FTP.	8.8	More Details
CVE-2020-4000	The SD-WAN Orchestrator 3.3.2 prior to 3.3.2 P3, 3.4.x prior to 3.4.4, and 4.0.x prior to 4.0.1 allows for executing files through directory traversal. An authenticated SD-WAN Orchestrator user is able to traversal directories which may lead to code execution of files.	8.8	More Details
CVE-2020-7563	A CWE-787: Out-of-bounds Write vulnerability exists in the Web Server on Modicon M340, Modicon Quantum and Modicon Premium Legacy offers and their Communication Modules (see notification for details) which could cause corruption of data, a crash, or code execution when uploading a specially crafted file on the controller over FTP.	8.8	More Details
CVE-2020-28579	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an authenticated, remote attacker to send a specially crafted HTTP message and achieve remote code execution with elevated privileges.	8.8	More Details
CVE-2020-24297	httpd on TP-Link TL-WPA4220 devices (versions 2 through 4) allows remote authenticated users to execute arbitrary OS commands by sending crafted POST requests to the endpoint /admin/powerline. Fixed version: TL-WPA4220(EU)_V4_201023	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26072	A vulnerability in the SOAP API of Cisco IoT Field Network Director (FND) could allow an authenticated, remote attacker to access and modify information on devices that belong to a different domain. The vulnerability is due to insufficient authorization in the SOAP API. An attacker could exploit this vulnerability by sending SOAP API requests to affected devices for devices that are outside their authorized domain. A successful exploit could allow the attacker to access and modify information on devices that belong to a different domain.	8.7	More Details
CVE-2020-4004	VMware ESXi (7.0 before ESXi70U1b-17168206, 6.7 before ESXi670-202011101-SG, 6.5 before ESXi650-202011301-SG), Workstation (15.x before 15.5.7), Fusion (11.x before 11.5.7) contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.	8.2	More Details
CVE-2020-13356	An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.8.9. A specially crafted request could bypass Multipart protection and read files in certain specific paths on the server. Affected versions are: >=8.8.9, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.	8.2	More Details
CVE-2020-7562	A CWE-125: Out-of-Bounds Read vulnerability exists in the Web Server on Modicon M340, Modicon Quantum and Modicon Premium Legacy offers and their Communication Modules (see notification for details) which could cause a segmentation fault or a buffer overflow when uploading a specially crafted file on the controller over FTP.	8.1	More Details
CVE-2020-26226	In the npm package semantic-release before version 17.2.3, secrets that would normally be masked by `semantic-release` can be accidentally disclosed if they contain characters that become encoded when included in a URL. Secrets that do not contain characters that become encoded when included in a URL are already masked properly. The issue is fixed in version 17.2.3.	8.1	More Details
CVE-2020-7927	Specially crafted API calls may allow an authenticated user who holds Organization Owner privilege to obtain an API key with Global Role privilege. This issue affects MongoDB Ops Manager v4.2 versions prior to and including 4.2.17, MongoDB Ops Manager v4.3 versions prior to and including 4.3.9 and MongoDB Ops Manager v4.4 versions prior to and including 4.4.2.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26228	TYPO3 is an open source PHP based web content management system. In TYPO3 before versions 9.5.23 and 10.4.10 user session identifiers were stored in cleartext - without processing with additional cryptographic hashing algorithms. This vulnerability cannot be exploited directly and occurs in combination with a chained attack - like for instance SQL injection in any other component of the system. Update to TYPO3 versions 9.5.23 or 10.4.10 that fix the problem described.	8.1	More Details
CVE-2019-14586	Use after free vulnerability in EDK II may allow an authenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via adjacent access.	8.0	More Details
CVE-2020-7553	A CWE-787 Out-of-bounds Write vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.	7.8	More Details
CVE-2020-7552	A CWE-787: Out-of-bounds Write vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247, that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.	7.8	More Details
CVE-2020-7551	A CWE-787: Out-of-bounds Write vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247, that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.	7.8	More Details
CVE-2020-28949	Archive_Tar through 1.4.10 has :// filename sanitization only to address phar attacks, and thus any other stream-wrapper attack (such as file:// to overwrite files) can still succeed.	7.8	More Details
CVE-2020-28211	A CWE-863: Incorrect Authorization vulnerability exists in PLC Simulator on EcoStruxure[a] Control Expert (now Unity Pro) (all versions) that could cause bypass of authentication when overwriting memory using a debugger.	7.8	More Details
CVE-2020-7544	A CWE-269 Improper Privilege Management vulnerability exists in EcoStruxure[a] Operator Terminal Expert runtime (Vijeo XD) that could cause privilege escalation on the workstation when interacting directly with a driver installed by the runtime software of EcoStruxure[a] Operator Terminal Expert.	7.8	More Details
CVE-2020-5674	Untrusted search path vulnerability in the installers of multiple SEIKO EPSON products allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28948	Archive_Tar through 1.4.10 allows an unserialization attack because phar: is blocked but PHAR: is not blocked.	7.8	More Details
CVE-2020-7554	A CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.	7.8	More Details
CVE-2020-7550	A CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 and prior that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.	7.8	More Details
CVE-2020-19667	Stack-based buffer overflow and unconditional jump in ReadXPMImage in coders/xpm.c in ImageMagick 7.0.10-7.	7.8	More Details
CVE-2020-7555	A CWE-787 Out-of-bounds Write vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.	7.8	More Details
CVE-2020-7556	A CWE-787 Out-of-bounds Write vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.	7.8	More Details
CVE-2018-16719	In Jingyun Antivirus v2.4.2.39, the driver file (hookbody.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x00221482.	7.8	More Details
CVE-2018-16720	In Jingyun Antivirus v2.4.2.39, the driver file (ZySandbox.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x1236001c, a related issue to CVE-2018-16304.	7.8	More Details
CVE-2018-16721	In Jingyun Antivirus v2.4.2.39, the driver file (ZySandbox.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x12360090, a related issue to CVE-2018-16306.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14575	Logic issue in DxeImageVerificationHandler() for EDK II may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2019-14563	Integer truncation in EDK II may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-28421	CA Unified Infrastructure Management 20.1 and earlier contains a vulnerability in the robot (controller) component that allows local attackers to elevate privileges.	7.8	More Details
CVE-2018-16722	In Jingyun Antivirus v2.4.2.39, the driver file (ZySandbox.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x12360094, a related issue to CVE-2018-16305.	7.8	More Details
CVE-2018-16723	In Jingyun Antivirus v2.4.2.39, the driver file (ZySandbox.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x12364020.	7.8	More Details
CVE-2020-27985	Security Onion v2 prior to 2.3.10 has an incorrect sudo configuration, which allows the administrative user to obtain root access without using the sudo password by editing and executing /home/<user>/SecurityOnion/setup/so-setup.	7.8	More Details
CVE-2020-4005	VMware ESXi (7.0 before ESXi70U1b-17168206, 6.7 before ESXi670-202011101-SG, 6.5 before ESXi650-202011301-SG) contains a privilege-escalation vulnerability that exists in the way certain system calls are being managed. A malicious actor with privileges within the VMX process only, may escalate their privileges on the affected system. Successful exploitation of this issue is only possible when chained with another vulnerability (e.g. CVE-2020-4004)	7.8	More Details
CVE-2020-28845	A CSV injection vulnerability in the Admin portal for Netskope 75.0 allows an unauthenticated user to inject malicious payload in admin's portal thus leads to compromise admin's system.	7.8	More Details
CVE-2020-20740	PDFResurrect before 0.20 lack of header validation checks causes heap-buffer-overflow in pdf_get_version().	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4739	IBM DB2 Accessories Suite for Linux, UNIX, and Windows, DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 188149.	7.8	More Details
CVE-2020-7558	A CWE-787 Out-of-bounds Write vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.	7.8	More Details
CVE-2020-7557	A CWE-125 Out-of-bounds Read vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.	7.8	More Details
CVE-2020-4701	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges.	7.8	More Details
CVE-2020-25989	Privilege escalation via arbitrary file write in pritunl electron client 1.0.1116.6 through v1.2.2550.20. Successful exploitation of the issue may allow an attacker to execute code on the effected system with root privileges.	7.8	More Details
CVE-2020-15301	SuiteCRM through 7.11.13 allows CSV Injection via registration fields in the Accounts, Contacts, Opportunities, and Leads modules. These fields are mishandled during a Download Import File Template operation.	7.8	More Details
CVE-2020-28572	A vulnerability in Trend Micro Apex One could allow an unprivileged user to abuse the product installer to reinstall the agent with additional malicious code in the context of a higher privilege.	7.8	More Details
CVE-2020-3367	A vulnerability in the log subscription subsystem of Cisco AsyncOS for the Cisco Secure Web Appliance (formerly Web Security Appliance) could allow an authenticated, local attacker to perform command injection and elevate privileges to root. This vulnerability is due to insufficient validation of user-supplied input for the web interface and CLI. An attacker could exploit this vulnerability by authenticating to the affected device and injecting scripting commands in the scope of the log subscription subsystem. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27696	Trend Micro Security 2020 (Consumer) contains a vulnerability in the installer package that could be exploited by placing a specific Windows system directory which can lead to obtaining administrative privileges during the installation of the product.	7.8	More Details
CVE-2020-27697	Trend Micro Security 2020 (Consumer) contains a vulnerability in the installer package that could be exploited by placing a malicious DLL in a non-protected location with high privileges (symlink attack) which can lead to obtaining administrative privileges during the installation of the product.	7.8	More Details
CVE-2020-27695	Trend Micro Security 2020 (Consumer) contains a vulnerability in the installer package that could be exploited by placing a malicious DLL in a local directory which can lead to obtaining administrative privileges during the installation of the product.	7.8	More Details
CVE-2020-26239	Scratch Addons is a WebExtension that supports both Chrome and Firefox. Scratch Addons before version 1.3.2 is vulnerable to DOM-based XSS. If the victim visited a specific website, the More Links addon of the Scratch Addons extension used incorrect regular expression which caused the HTML-escaped values to be unescaped, leading to XSS. Scratch Addons version 1.3.2 fixes the bug. The extension will be automatically updated by the browser. More Links addon can be disabled via the option of the extension.	7.6	More Details
CVE-2020-13359	The Terraform API in GitLab CE/EE 12.10+ exposed the object storage signed URL on the delete operation allowing a malicious project maintainer to overwrite the Terraform state, bypassing audit and other business controls. Affected versions are >=12.10, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.	7.6	More Details
CVE-2020-28574	A unauthenticated path traversal arbitrary remote file deletion vulnerability in Trend Micro Worry-Free Business Security 10 SP1 could allow an unauthenticated attacker to exploit the vulnerability and modify or delete arbitrary files on the product's management console.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26236	In ScratchVerifier before commit a603769, an attacker can hijack the verification process to log into someone else's account on any site that uses ScratchVerifier for logins. A possible exploitation would follow these steps: 1. User starts login process. 2. Attacker attempts login for user, and is given the same verification code. 3. User comments code as part of their normal login. 4. Before user can, attacker completes the login process now that the code is commented. 5. User gets a failed login and attacker now has control of the account. Since commit a603769 starting a login twice will generate different verification codes, causing both user and attacker login to fail. For clients that rely on a clone of ScratchVerifier not hosted by the developers, their users may attempt to finish the login process as soon as possible after commenting the code. There is no reliable way for the attacker to know before the user can finish the process that the user has commented the code, so this vulnerability only really affects those who comment the code and then take several seconds before finishing the login.	7.5	More Details
CVE-2020-7559	A CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability exists in PLC Simulator on EcoStruxure[a] Control Expert (now Unity Pro) (all versions) that could cause a crash of the PLC simulator present in EcoStruxure[a] Control Expert software when receiving a specially crafted request over Modbus.	7.5	More Details
CVE-2020-26890	Matrix Synapse before 1.20.0 erroneously permits non-standard NaN, Infinity, and -Infinity JSON values in fields of m.room.member events, allowing remote attackers to execute a denial of service attack against the federation and common Matrix clients. If such a malformed event is accepted into the room's state, the impact is long-lasting and is not fixed by an upgrade to a newer version, requiring the event to be manually redacted instead. Since events are replicated to servers of other room members, the impact is not constrained to the server of the event sender.	7.5	More Details
CVE-2020-25696	A flaw was found in the psql interactive terminal of PostgreSQL in versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. If an interactive psql session uses \gset when querying a compromised server, the attacker can execute arbitrary code as the operating system account running psql. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3392	A vulnerability in the API of Cisco IoT Field Network Director (FND) could allow an unauthenticated, remote attacker to view sensitive information on an affected system. The vulnerability exists because the affected software does not properly authenticate API calls. An attacker could exploit this vulnerability by sending API requests to an affected system. A successful exploit could allow the attacker to view sensitive information on the affected system, including information about the devices that the system manages, without authentication.	7.5	More Details
CVE-2020-5668	Uncontrolled resource consumption vulnerability in MELSEC iQ-R Series modules (R00/01/02CPU firmware version '19' and earlier, R04/08/16/32/120 (EN) CPU firmware version '51' and earlier, R08/16/32/120SFCPU firmware version '22' and earlier, R08/16/32/120PCPU firmware version '25' and earlier, R08/16/32/120PSFCPU firmware version '06' and earlier, RJ71EN71 firmware version '47' and earlier, RJ71GF11-T2 firmware version '47' and earlier, RJ72GF15-T2 firmware version '07' and earlier, RJ71GP21-SX firmware version '47' and earlier, RJ71GP21S-SX firmware version '47' and earlier, and RJ71GN11-T2 firmware version '11' and earlier) allows a remote unauthenticated attacker to cause an error in a CPU unit and cause a denial-of-service (DoS) condition in execution of the program and its communication, or to cause a denial-of-service (DoS) condition in communication via the unit by receiving a specially crafted SLMP packet	7.5	More Details
CVE-2020-7538	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in PLC Simulator on EcoStruxure[a] Control Expert (now Unity Pro) (all versions) that could cause a crash of the PLC simulator present in EcoStruxure[a] Control Expert software when receiving a specially crafted request over Modbus.	7.5	More Details
CVE-2020-4937	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.0.3.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 191814.	7.5	More Details
CVE-2020-13355	An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.14. A path traversal is found in LFS Upload that allows attacker to overwrite certain specific paths on the server. Affected versions are: >=8.14, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2.	7.5	More Details
CVE-2019-20925	An unauthenticated client can trigger denial of service by issuing specially crafted wire protocol messages, which cause the message decompressor to incorrectly allocate memory. This issue affects MongoDB Server v4.2 versions prior to 4.2.1; MongoDB Server v4.0 versions prior to 4.0.13; MongoDB Server v3.6 versions prior to 3.6.15 and MongoDB Server v3.4 versions prior to 3.4.24.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26076	A vulnerability in Cisco IoT Field Network Director (FND) could allow an unauthenticated, remote attacker to view sensitive database information on an affected device. The vulnerability is due to the absence of authentication for sensitive information. An attacker could exploit this vulnerability by sending crafted curl commands to an affected device. A successful exploit could allow the attacker to view sensitive database information on the affected device.	7.5	More Details
CVE-2020-24227	Playground Sessions v2.5.582 (and earlier) for Windows, stores the user credentials in plain text allowing anyone with access to UserProfiles.sol to extract the email and password.	7.5	More Details
CVE-2020-14230	HCL Domino is susceptible to a Denial of Service vulnerability caused by improper validation of user-supplied input. A remote unauthenticated attacker could exploit this vulnerability using a specially-crafted email message to hang the server. Versions previous to releases 9.0.1 FP10 IF6, 10.0.1 FP5 and 11.0.1 are affected.	7.5	More Details
CVE-2020-14234	HCL Domino is susceptible to a Denial of Service vulnerability due to improper validation of user-supplied input, potentially giving an attacker the ability to crash the server. Versions previous to release 9.0.1 FP10 IF6 and release 10.0.1 are affected.	7.5	More Details
CVE-2020-14258	HCL Notes is susceptible to a Denial of Service vulnerability caused by improper validation of user-supplied input. A remote unauthenticated attacker could exploit this vulnerability using a specially-crafted email message to hang the client. Versions 9, 10 and 11 are affected.	7.5	More Details
CVE-2020-28975	svm_predict_values in svm.cpp in Libsvm v324, as used in scikit-learn 0.23.2 and other products, allows attackers to cause a denial of service (segmentation fault) via a crafted model SVM (introduced via pickle, json, or any other model permanence standard) with a large value in the _n_support array. NOTE: the scikit-learn vendor's position is that the behavior can only occur if the library's API is violated by an application that changes a private attribute.	7.5	More Details
CVE-2020-28367	Code injection in the go command with cgo before Go 1.14.12 and Go 1.15.5 allows arbitrary code execution at build time via malicious gcc flags specified via a #cgo directive.	7.5	More Details
CVE-2020-7925	Incorrect validation of user input in the role name parser may lead to use of uninitialized memory allowing an unauthenticated attacker to use a specially crafted request to cause a denial of service. This issue affects MongoDB Server v4.4 versions prior to 4.4.0-rc12; MongoDB Server v4.2 versions prior to 4.2.9.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14559	Uncontrolled resource consumption in EDK II may allow an unauthenticated user to potentially enable denial of service via network access.	7.5	More Details
CVE-2020-28366	Code injection in the go command with cgo before Go 1.14.12 and Go 1.15.5 allows arbitrary code execution at build time via a malicious unquoted symbol name in a linked object file.	7.5	More Details
CVE-2020-28362	Go before 1.14.12 and 1.15.x before 1.15.4 allows Denial of Service.	7.5	More Details
CVE-2020-28091	cxuucms v3 has a SQL injection vulnerability, which can lead to the leakage of all database data via the keywords parameter via search.php.	7.5	More Details
CVE-2020-29057	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. It allows remote attackers to cause a denial of service (reboot) by sending random bytes to the telnet server on port 23, aka a "shawarma" attack.	7.5	More Details
CVE-2020-29063	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. A custom encryption algorithm is used to store encrypted passwords. This algorithm will XOR the password with the hardcoded *j7a(L#yZ98sSd5HfSgGjMj8;Ss;d)(*&^#@$a2s0i3g value.	7.5	More Details
CVE-2015-9550	An issue was discovered on TOTOLINK A850R-V1 through 1.0.1-B20150707.1612 and F1-V2 through 1.1-B20150708.1646 devices. By sending a specific hel,xasf packet to the WAN interface, it is possible to open the web management interface on the WAN interface.	7.5	More Details
CVE-2020-15246	October is a free, open-source, self-hosted CMS platform based on the Laravel PHP Framework. In October CMS from version 1.0.421 and before version 1.0.469, an attacker can read local files on an October CMS server via a specially crafted request. Issue has been patched in Build 469 (v1.0.469) and v1.1.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25698	Users' enrollment capabilities were not being sufficiently checked in Moodle when they are restored into an existing course. This could lead to them unenrolling users without having permission to do so. Versions affected: 3.5 to 3.5.14, 3.7 to 3.7.8, 3.8 to 3.8.5, 3.9 to 3.9.2 and earlier unsupported versions. Fixed in 3.9.3, 3.8.6, 3.7.9, 3.5.15, and 3.10.	7.5	More Details
CVE-2020-28924	An issue was discovered in Rclone before 1.53.3. Due to the use of a weak random number generator, the password generator has been producing weak passwords with much less entropy than advertised. The suggested passwords depend deterministically on the time the second rclone was started. This limits the entropy of the passwords enormously. These passwords are often used in the crypt backend for encryption of data. It would be possible to make a dictionary of all possible passwords with about 38 million entries per password length. This would make decryption of secret material possible with a plausible amount of effort. NOTE: all passwords generated by affected versions should be changed.	7.5	More Details
CVE-2020-28331	Barco wePresent WiPG-1600W devices have Improper Access Control. Affected Version(s): 2.5.1.8. The Barco wePresent WiPG-1600W device has an SSH daemon included in the firmware image. By default, the SSH daemon is disabled and does not start at system boot. The system initialization scripts read a device configuration file variable to see if the SSH daemon should be started. The web interface does not provide a visible capability to alter this configuration file variable. However, a malicious actor can include this variable in a POST such that the SSH daemon will be started when the device boots.	7.5	More Details
CVE-2020-8277	A Node.js application that allows an attacker to trigger a DNS request for a host of their choice could trigger a Denial of Service in versions < 15.2.1, < 14.15.1, and < 12.19.1 by getting the application to resolve a DNS record with a larger number of responses. This is fixed in 15.2.1, 14.15.1, and 12.19.1.	7.5	More Details
CVE-2020-12593	Symantec Endpoint Detection & Response, prior to 4.5, may be susceptible to an information disclosure issue, which is a type of vulnerability that could potentially allow unauthorized access to data.	7.5	More Details
CVE-2019-12412	A flaw in the libapreq2 v2.07 to v2.13 multipart parser can deference a null pointer leading to a process crash. A remote attacker could send a request causing a process crash which could lead to a denial of service attack.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28054	JamoDat TSMManager Collector version up to 6.5.0.21 is vulnerable to an Authorization Bypass because the Collector component is not properly validating an authenticated session with the Viewer. If the Viewer has been modified (binary patched) and the Bypass Login functionality is being used, an attacker can request every Collector's functionality as if they were a properly logged-in user: administrating connected instances, reviewing logs, editing configurations, accessing the instances' consoles, accessing hardware configurations, etc.Exploiting this vulnerability won't grant an attacker access nor control on remote ISP servers as no credentials is sent with the request.	7.5	More Details
CVE-2020-25699	In moodle, insufficient capability checks could lead to users with the ability to course restore adding additional capabilities to roles within that course. Versions affected: 3.9 to 3.9.2, 3.8 to 3.8.5, 3.7 to 3.7.8, 3.5 to 3.5.14 and earlier unsupported versions. This is fixed in moodle 3.9.3, 3.8.6, 3.7.9, 3.5.15, and 3.10.	7.5	More Details
CVE-2020-8279	Missing validation of server certificates for out-going connections in Nextcloud Social < 0.4.0 allowed a man-in-the-middle attack.	7.4	More Details
CVE-2020-25406	app\admin\controller\sys\Uploads.php in lemocms 1.8.x allows users to upload files to upload executable files.	7.3	More Details
CVE-2020-7565	A CWE-326: Inadequate Encryption Strength vulnerability exists in Modicon M221 (all references, all versions) that could allow the attacker to break the encryption key when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M221 controller.	7.3	More Details
CVE-2020-7566	A CWE-334: Small Space of Random Values vulnerability exists in Modicon M221 (all references, all versions) that could allow the attacker to break the encryption keys when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M221 controller.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12510	The default installation path of the TwinCAT XAR 3.1 software in all versions is underneath C:\TwinCAT. If the directory does not exist it and further subdirectories are created with permissions which allow every local user to modify the content. The default installation registers TcSysUI.exe for automatic execution upon log in of a user. If a less privileged user has a local account he or she can replace TcSysUI.exe. It will be executed automatically by another user during login. This is also true for users with administrative access. Consequently, a less privileged user can trick a higher privileged user into executing code he or she modified this way. By default Beckhoff's IPCs are shipped with TwinCAT software installed this way and with just a single local user configured. Thus the vulnerability exists if further less privileged users have been added.	7.3	More Details
CVE-2020-25654	An ACL bypass flaw was found in pacemaker. An attacker having a local account on the cluster and in the haclient group could use IPC communication with various daemons directly to perform certain tasks that they would be prevented by ACLs from doing if they went through the configuration.	7.2	More Details
CVE-2020-28580	A command injection vulnerability in AddVLANItem of Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an authenticated, remote attacker to send specially crafted HTTP messages and execute arbitrary OS commands with elevated privileges.	7.2	More Details
CVE-2020-26933	Trusted Computing Group (TCG) Trusted Platform Module Library Family 2.0 Library Specification Revisions 1.38 through 1.59 has Incorrect Access Control during a non-orderly TPM shut-down that uses USE_DA_USED. Improper initialization of this shut-down may result in susceptibility to a dictionary attack.	7.2	More Details
CVE-2020-7777	This affects all versions of package jsen. If an attacker can control the schema file, it could run arbitrary JavaScript code on the victim machine. In the module description and README file there is no mention about the risks of untrusted schema files, so I assume that this is applicable. In particular the required field of the schema is not properly sanitized. The resulting string that is build based on the schema definition is then passed to a Function.apply();, leading to an Arbitrary Code Execution.	7.2	More Details
CVE-2020-4002	The SD-WAN Orchestrator 3.3.2 prior to 3.3.2 P3, 3.4.x prior to 3.4.4, and 4.0.x prior to 4.0.1 handles system parameters in an insecure way. An authenticated SD-WAN Orchestrator user with high privileges may be able to execute arbitrary code on the underlying operating system.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28581	A command injection vulnerability in ModifyVLANItem of Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an authenticated, remote attacker to send specially crafted HTTP messages and execute arbitrary OS commands with elevated privileges.	7.2	More Details
CVE-2020-9049	A vulnerability in specified versions of American Dynamics victor Web Client and Software House C•CURE Web Client could allow an unauthenticated attacker on the network to create and sign their own JSON Web Token and use it to execute an HTTP API Method without the need for valid authentication/authorization. Under certain circumstances, this could be used by an attacker to impact system availability by conducting a Denial of Service attack.	7.1	More Details
CVE-2020-28209	A CWE-428 Windows Unquoted Search Path vulnerability exists in EcoStruxure Building Operation Enterprise Server installer V1.9 - V3.1 and Enterprise Central installer V2.0 - V3.1 that could cause any local Windows user who has write permission on at least one of the subfolders of the Connect Agent service binary path, being able to gain the privilege of the user who started the service. By default, the Enterprise Server and Enterprise Central is always installed at a location requiring Administrator privileges so the vulnerability is only valid if the application has been installed on a non-secure location.	7.0	More Details
CVE-2020-13799	Western Digital has identified a security vulnerability in the Replay Protected Memory Block (RPMB) protocol as specified in multiple standards for storage device interfaces, including all versions of eMMC, UFS, and NVMe. The RPMB protocol is specified by industry standards bodies and is implemented by storage devices from multiple vendors to assist host systems in securing trusted firmware. Several scenarios have been identified in which the RPMB state may be affected by an attacker without the knowledge of the trusted component that uses the RPMB feature.	6.8	More Details
CVE-2020-15436	Use-after-free vulnerability in fs/block_dev.c in the Linux kernel before 5.8 allows local users to gain privileges or cause a denial of service by leveraging improper access to a certain error field.	6.7	More Details
CVE-2018-20802	A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries with compound indexes affecting QueryPlanner. This issue affects MongoDB Server v3.6 versions prior to 3.6.9 and MongoDB Server v4.0 versions prior to 4.0.3.	6.5	More Details
CVE-2020-12352	Improper access control in BlueZ may allow an unauthenticated user to potentially enable information disclosure via adjacent access.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7926	A user authorized to perform database queries may cause denial of service by issuing a specially crafted query which violates an invariant in the server selection subsystem. This issue affects MongoDB Server v4.4 versions prior to 4.4.1. Versions before 4.4 are not affected.	6.5	More Details
CVE-2018-20804	A user authorized to perform database queries may trigger denial of service by issuing specially crafted applyOps invocations. This issue affects MongoDB Server v4.0 versions prior to 4.0.10 and MongoDB Server v3.6 versions prior to 3.6.13.	6.5	More Details
CVE-2018-20803	A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries, which loop indefinitely in mathematics processing while retaining locks. This issue affects MongoDB Server v4.0 versions prior to 4.0.5; MongoDB Server v3.6 versions prior to 3.6.10 and MongoDB Server v3.4 versions prior to 3.4.19.	6.5	More Details
CVE-2020-24815	A Server-Side Request Forgery (SSRF) affecting the PDF generation in MicroStrategy 10.4, 2019 before Update 6, and 2020 before Update 2 allows authenticated users to access the content of internal network resources or leak files from the local system via HTML containers embedded in a dossier/dashboard document. NOTE: 10.4., no fix will be released as version will reach end-of-life on 31/12/2020.	6.5	More Details
CVE-2020-28053	HashiCorp Consul and Consul Enterprise 1.2.0 up to 1.8.5 allowed operators with operator:read ACL permissions to read the Connect CA private key configuration. Fixed in 1.6.10, 1.7.10, and 1.8.6.	6.5	More Details
CVE-2019-20924	A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries which trigger an invariant in the IndexBoundsBuilder. This issue affects MongoDB Server v4.2 versions prior to 4.2.2.	6.5	More Details
CVE-2018-20805	A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries, which perform an $elemMatch . This issue affects MongoDB Server v4.0 versions prior to 4.0.5 and MongoDB Server v3.6 versions prior to 3.6.10.	6.5	More Details
CVE-2019-20923	A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries, which throw unhandled Javascript exceptions containing types intended to be scoped to the Javascript engine's internals. This issue affects MongoDB Server v4.0 versions prior to 4.0.7.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-2392	A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries, which use the $mod operator to overflow negative values. This issue affects: MongoDB Inc. MongoDB Server v4.4 versions prior to 4.4.1; v4.2 versions prior to 4.2.9; v4.0 versions prior to 4.0.20; v3.6 versions prior to 3.6.20.	6.5	More Details
CVE-2019-2393	A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries, which use $lookup and collations. This issue affects MongoDB Server v4.2 versions prior to 4.2.1; MongoDB Server v4.0 versions prior to 4.0.13 and MongoDB Server v3.6 versions prior to 3.6.15.	6.5	More Details
CVE-2020-4003	VMware SD-WAN Orchestrator 3.3.2 prior to 3.3.2 P3, 3.4.x prior to 3.4.4, and 4.0.x prior to 4.0.1 was found to be vulnerable to SQL-injection attacks allowing for potential information disclosure. An authenticated SD-WAN Orchestrator user may inject code into SQL queries which may lead to information disclosure.	6.5	More Details
CVE-2020-28005	httpd on TP-Link TL-WPA4220 devices (hardware versions 2 through 4) allows remote authenticated users to trigger a buffer overflow (causing a denial of service) by sending a POST request to the /admin/syslog endpoint. Fixed version: TL-WPA4220(EU)_V4_201023	6.5	More Details
CVE-2019-14587	Logic issue EDK II may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2020-7928	A user authorized to perform database queries may trigger a read overrun and access arbitrary memory by issuing specially crafted queries. This issue affects MongoDB Server v4.4 versions prior to 4.4.1; MongoDB Server v4.2 versions prior to 4.2.9; MongoDB Server v4.0 versions prior to 4.0.20 and MongoDB Server v3.6 versions prior to 3.6.20.	6.5	More Details
CVE-2020-3482	A vulnerability in the Traversal Using Relays around NAT (TURN) server component of Cisco Expressway software could allow an unauthenticated, remote attacker to bypass security controls and send network traffic to restricted destinations. The vulnerability is due to improper validation of specific connection information by the TURN server within the affected software. An attacker could exploit this issue by sending specially crafted network traffic to the affected software. A successful exploit could allow the attacker to send traffic through the affected software to destinations beyond the application, possibly allowing the attacker to gain unauthorized network access.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28917	An issue was discovered in the view_statistics (aka View frontend statistics) extension before 2.0.1 for TYPO3. It saves all GET and POST data of TYPO3 frontend requests to the database. Depending on the extensions used on a TYPO3 website, sensitive data (e.g., cleartext passwords if ext:felogin is installed) may be saved.	6.5	More Details
CVE-2020-25700	In moodle, some database module web services allowed students to add entries within groups they did not belong to. Versions affected: 3.9 to 3.9.2, 3.8 to 3.8.5, 3.7 to 3.7.8, 3.5 to 3.5.14 and earlier unsupported versions. This is fixed in moodle 3.8.6, 3.7.9, 3.5.15, and 3.10.	6.5	More Details
CVE-2020-28348	HashiCorp Nomad and Nomad Enterprise 0.9.0 up to 0.12.7 client Docker file sandbox feature may be subverted when not explicitly disabled or when using a volume mount type. Fixed in 0.12.8, 0.11.7, and 0.10.8.	6.5	More Details
CVE-2020-5641	Cross-site request forgery (CSRF) vulnerability in GS108Ev3 firmware version 2.06.10 and earlier allows remote attackers to hijack the authentication of administrators and the product's settings may be changed without the user's intention or consent via unspecified vectors.	6.5	More Details
CVE-2020-25472	SimplePHPscripts News Script PHP Pro 2.3 is affected by a Cross Site Request Forgery (CSRF) vulnerability, which allows attackers to add new users.	6.5	More Details
CVE-2020-7573	A CWE-284 Improper Access Control vulnerability exists in EcoStruxure Building Operation WebReports V1.9 - V3.1 that could cause a remote attacker being able to access a restricted web resources due to improper access control.	6.5	More Details
CVE-2020-12496	Endress+Hauser Ecograph T (Neutral/Private Label) (RSG35, ORSG35) and Memograph M (Neutral/Private Label) (RSG45, ORSG45) with Firmware version V2.0.0 and above is prone to exposure of sensitive information to an unauthorized actor. The firmware release has a dynamic token for each request submitted to the server, which makes repeating requests and analysis complex enough. Nevertheless, it's possible and during the analysis it was discovered that it also has an issue with the access-control matrix on the server-side. It was found that a user with low rights can get information from endpoints that should not be available to this user.	6.5	More Details
CVE-2020-25473	SimplePHPscripts News Script PHP Pro 2.3 does not properly set the HttpOnly Flag from Session Cookies.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19668	Unverified indexs into the array lead to out of bound access in the gif_out_code function in fromgif.c in libsixel 1.8.6.	6.5	More Details
CVE-2020-3419	A vulnerability in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to join a Webex session without appearing on the participant list. This vulnerability is due to improper handling of authentication tokens by a vulnerable Webex site. An attacker could exploit this vulnerability by sending crafted requests to a vulnerable Cisco Webex Meetings or Cisco Webex Meetings Server site. A successful exploit requires the attacker to have access to join a Webex meeting, including applicable meeting join links and passwords. The attacker could then exploit this vulnerability to join meetings, without appearing in the participant list, while having full access to audio, video, chat, and screen sharing capabilities.	6.5	More Details
CVE-2020-28330	Barco wePresent WiPG-1600W devices have Unprotected Transport of Credentials. Affected Version(s): 2.5.1.8. An attacker armed with hardcoded API credentials (retrieved by exploiting CVE-2020-28329) can issue an authenticated query to display the admin password for the main web user interface listening on port 443/tcp of a Barco wePresent WiPG-1600W device.	6.5	More Details
CVE-2020-26078	A vulnerability in the file system of Cisco IoT Field Network Director (FND) could allow an authenticated, remote attacker to overwrite files on an affected system. The vulnerability is due to insufficient file system protections. An attacker could exploit this vulnerability by crafting API requests and sending them to an affected system. A successful exploit could allow the attacker to overwrite files on an affected system.	6.5	More Details
CVE-2020-3984	The SD-WAN Orchestrator 3.3.2 prior to 3.3.2 P3 and 3.4.x prior to 3.4.4 does not apply correct input validation which allows for SQL-injection. An authenticated SD-WAN Orchestrator user may exploit a vulnerable API call using specially crafted SQL queries which may lead to unauthorized data access.	6.5	More Details
CVE-2020-3471	A vulnerability in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to maintain bidirectional audio despite being expelled from an active Webex session. The vulnerability is due to a synchronization issue between meeting and media services on a vulnerable Webex site. An attacker could exploit this vulnerability by sending crafted requests to a vulnerable Cisco Webex Meetings or Cisco Webex Meetings Server site. A successful exploit could allow the attacker to maintain the audio connection of a Webex session despite being expelled.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4592	IBM MQ Appliance 9.1.CD and LTS could allow an authenticated user, under nondefault configuration to cause a data corruption attack due to an error when using segmented messages.	6.5	More Details
CVE-2020-7842	Improper Input validation vulnerability exists in Netis Korea D'live AP which could cause arbitrary command injection and execution when the time setting (using ntpServerIp1 parameter) for the users. This affects D'live set-top box AP(WF2429TB) v1.1.10.	6.4	More Details
CVE-2020-28350	A Cross Site Scripting (XSS) vulnerability exists in OPAC in Sokrates SOWA SowaSQL through 5.6.1 via the sowacgi.php typ parameter.	6.1	More Details
CVE-2020-28724	Open redirect vulnerability in werkzeug before 0.11.6 via a double slash in the URL.	6.1	More Details
CVE-2020-28210	A CWE-79 Improper Neutralization of Input During Web Page Generation (Cross-site Scripting) vulnerability exists in EcoStruxure Building Operation WebStation V2.0 - V3.1 that could cause an attacker to inject HTML and JavaScript code into the user's browser.	6.1	More Details
CVE-2020-28927	There is a Stored XSS in Magicpin v2.1 in the User Registration section. Each time an admin visits the manage user section from the admin panel, the XSS triggers and the attacker can able to steal the cookie according to the crafted payload.	6.1	More Details
CVE-2020-26884	RSA Archer 6.8 through 6.8.0.3 and 6.9 contains a URL injection vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability by tricking a victim application user into executing malicious JavaScript code in the context of the web application.	6.1	More Details
CVE-2020-28726	Open redirect in SeedDMS 6.0.13 via the dropfolderfileform1 parameter to out/out.AddDocument.php.	6.1	More Details
CVE-2020-28947	In MISP 2.4.134, XSS exists in the template element index view because the id parameter is mishandled.	6.1	More Details
CVE-2020-26554	REDDOXX MailDepot 2033 (aka 2.3.3022) allows XSS via an incoming HTML e-mail message.	6.1	More Details
CVE-2020-15300	SuiteCRM through 7.11.13 has an Open Redirect in the Documents module via a crafted SVG document.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5797	UNIX Symbolic Link (Symlink) Following in TP-Link Archer C9(US)_V1_180125 firmware allows an unauthenticated actor, with physical access and network access, to read sensitive files and write to a limited set of files after plugging a crafted USB drive into the router.	6.1	More Details
CVE-2020-22394	In YzmCMS v5.5 the member contribution function in the editor contains a cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2020-27126	A vulnerability in an API of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks. The vulnerability is due to improper validation of user-supplied input to an application programmatic interface (API) within Cisco Webex Meetings. An attacker could exploit this vulnerability by convincing a targeted user to follow a link designed to submit malicious input to the API used by Cisco Webex Meetings. A successful exploit could allow the attacker to conduct cross-site scripting attacks and potentially gain access to sensitive browser-based information from the system of a targeted user.	6.1	More Details
CVE-2020-26081	Multiple vulnerabilities in the web UI of Cisco IoT Field Network Director (FND) could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against users on an affected system. The vulnerabilities are due to insufficient validation of user-supplied input that is processed by the web UI. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information on an affected system.	6.1	More Details
CVE-2020-25474	SimplePHPscripts News Script PHP Pro 2.3 is affected by a Cross Site Scripting (XSS) vulnerability via the editor_name parameter.	6.1	More Details
CVE-2020-26227	TYPO3 is an open source PHP based web content management system. In TYPO3 before versions 9.5.23 and 10.4.10 the system extension Fluid (typo3/cms-fluid) of the TYPO3 core is vulnerable to cross-site scripting passing user-controlled data as argument to Fluid view helpers. Update to TYPO3 versions 9.5.23 or 10.4.10 that fix the problem described.	6.1	More Details
CVE-2020-29053	HRSALE 2.0.0 allows XSS via the admin/project/projects_calendar set_date parameter.	6.1	More Details
CVE-2020-25702	In Moodle, it was possible to include JavaScript when re-naming content bank items. Versions affected: 3.9 to 3.9.2. This is fixed in moodle 3.9.3 and 3.10.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-22723	A cross-site scripting (XSS) vulnerability in Beijing Liangjing Zhicheng Technology Co., Ltd ljcmsshop version 1.14 allows remote attackers to inject arbitrary web script or HTML via user.php by registering an account directly in the user center, and then adding the payload to the delivery address.	6.1	More Details
CVE-2020-4783	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 189214.	5.9	More Details
CVE-2020-29055	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. By default, the appliance can be managed remotely only with HTTP, telnet, and SNMP. It doesn't support SSL/TLS for HTTP or SSH. An attacker can intercept passwords sent in cleartext and conduct man-in-the-middle attacks on the management of the appliance.	5.9	More Details
CVE-2020-28915	A buffer over-read (at the framebuffer layer) in the fbcon code in the Linux kernel before 5.8.15 could be used by local attackers to read kernel memory, aka CID-6735b4632def.	5.8	More Details
CVE-2020-26237	Highlight.js is a syntax highlighter written in JavaScript. Highlight.js versions before 9.18.2 and 10.1.2 are vulnerable to Prototype Pollution. A malicious HTML code block can be crafted that will result in prototype pollution of the base object's prototype during highlighting. If you allow users to insert custom HTML code blocks into your page/app via parsing Markdown code blocks (or similar) and do not filter the language names the user can provide you may be vulnerable. The pollution should just be harmless data but this can cause problems for applications not expecting these properties to exist and can result in strange behavior or application crashes, i.e. a potential DOS vector. If your website or application does not render user provided data it should be unaffected. Versions 9.18.2 and 10.1.2 and newer include fixes for this vulnerability. If you are using version 7 or 8 you are encouraged to upgrade to a newer release.	5.8	More Details
CVE-2020-7567	A CWE-311: Missing Encryption of Sensitive Data vulnerability exists in Modicon M221 (all references, all versions) that could allow the attacker to find the password hash when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M221 controller and broke the encryption keys.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0569	Out of bounds write in Intel(R) PROSet/Wireless WiFi products on Windows 10 may allow an authenticated user to potentially enable denial of service via local access.	5.7	More Details
CVE-2020-26068	A vulnerability in the xAPI service of Cisco Telepresence CE Software and Cisco RoomOS Software could allow an authenticated, remote attacker to generate an access token for an affected device. The vulnerability is due to insufficient access authorization. An attacker could exploit this vulnerability by using the xAPI service to generate a specific token. A successful exploit could allow the attacker to use the generated token to enable experimental features on the device that should not be available to users.	5.5	More Details
CVE-2020-28928	In musl libc through 1.2.1, wcsnrtombs mishandles particular combinations of destination buffer size and source character limit, as demonstrated by an invalid write access (buffer overflow).	5.5	More Details
CVE-2020-10763	An information-disclosure flaw was found in the way Heketi before 10.1.0 logs sensitive information. This flaw allows an attacker with local access to the Heketi server to read potentially sensitive information such as gluster-block passwords.	5.5	More Details
CVE-2020-10762	An information-disclosure flaw was found in the way that gluster-block before 0.5.1 logs the output from gluster-block CLI operations. This includes recording passwords to the cmd_history.log file which is world-readable. This flaw allows local users to obtain sensitive information by reading the log file. The highest threat from this vulnerability is to data confidentiality.	5.5	More Details
CVE-2020-28941	An issue was discovered in drivers/accessibility/speakup/spk_ttyio.c in the Linux kernel through 5.9.9. Local attackers on systems with the speakup driver could cause a local denial of service attack, aka CID-d41227544427. This occurs because of an invalid free when the line discipline is used more than once.	5.5	More Details
CVE-2019-14562	Integer overflow in DxeImageVerificationHandler() EDK II may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-29003	The PollNY extension for MediaWiki through 1.35 allows XSS via an answer option for a poll question, entered during Special:CreatePoll or Special:UpdatePoll.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4718	IBM Jazz Reporting Service 6.0.6, 6.0.6.1, 7.0, and 7.0.1 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 187731.	5.4	More Details
CVE-2020-14208	SuiteCRM 7.11.13 is affected by stored Cross-Site Scripting (XSS) in the Documents preview functionality. This vulnerability could allow remote authenticated attackers to inject arbitrary web script or HTML.	5.4	More Details
CVE-2020-25454	Cross-site Scripting (XSS) vulnerability in grocy 2.7.1 via the add recipe module, which gets executed when deleting the recipe.	5.4	More Details
CVE-2020-28361	Kamailio before 5.4.0, as used in Sip Express Router (SER) in Sippy Softswitch 4.5 through 5.2 and other products, allows a bypass of a header-removal protection mechanism via whitespace characters. This occurs in the remove_hf function in the Kamailio textops module. Particular use of remove_hf in Sippy Softswitch may allow skilled attacker having a valid credential in the system to disrupt internal call start/duration accounting mechanisms leading potentially to a loss of revenue.	5.4	More Details
CVE-2020-7571	A CWE-79 Multiple Improper Neutralization of Input During Web Page Generation (Cross-site Scripting Reflected) vulnerability exists in EcoStruxure Building Operation WebReports V1.9 - V3.1 that could cause a remote attacker to inject arbitrary web script or HTML due to incorrect sanitization of user supplied data and achieve a Cross-Site Scripting reflected attack against other WebReport users.	5.4	More Details
CVE-2020-7570	A CWE-79 Improper Neutralization of Input During Web Page Generation (Cross-site Scripting Stored) vulnerability exists in EcoStruxure Building Operation WebReports V1.9 - V3.1 that could cause an authenticated remote user being able to inject arbitrary web script or HTML due to incorrect sanitization of user-supplied data and achieve a Cross-Site Scripting stored attack against other WebReport users.	5.4	More Details
CVE-2020-25701	If the upload course tool in Moodle was used to delete an enrollment method which did not exist or was not already enabled, the tool would erroneously enable that enrollment method. This could lead to unintended users gaining access to the course. Versions affected: 3.9 to 3.9.2, 3.8 to 3.8.5, 3.7 to 3.7.8, 3.5 to 3.5.14 and earlier unsupported versions. This is fixed in moodle 3.9.3, 3.8.6, 3.7.9, 3.5.15, and 3.10.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4771	IBM Spectrum Protect Operations Center 8.1.0.000 through 8.1.10.and 7.1.0.000 through 7.1.11 could allow a remote attacker to obtain sensitive information, caused by improper authentication of a websocket endpoint. By using known tools to subscribe to the websocket event stream, an attacker could exploit this vulnerability to obtain sensitive information. IBM X-Force ID: 188993.	5.3	More Details
CVE-2020-25703	The participants table download in Moodle always included user emails, but should have only done so when users' emails are not hidden. Versions affected: 3.9 to 3.9.2, 3.8 to 3.8.5 and 3.7 to 3.7.8. This is fixed in moodle 3.9.3, 3.8.6, 3.7.9, and 3.10.	5.3	More Details
CVE-2020-28896	Mutt before 2.0.2 and NeoMutt before 2020-11-20 did not ensure that $ssl_force_tls was processed if an IMAP server's initial server response was invalid. The connection was not properly closed, and the code could continue attempting to authenticate. This could result in authentication credentials being exposed on an unencrypted connection, or to a machine-in-the-middle.	5.3	More Details
CVE-2020-25640	A flaw was discovered in WildFly before 21.0.0.Final where, Resource adapter logs plain text JMS password at warning level on connection error, inserting sensitive information in the log file.	5.3	More Details
CVE-2020-28954	web/controllers/ApiController.groovy in BigBlueButton before 2.2.29 lacks certain parameter sanitization, as demonstrated by accepting control characters in a user name.	5.3	More Details
CVE-2020-15710	Potential double free in Bluez 5 module of PulseAudio could allow a local attacker to leak memory or crash the program. The modargs variable may be freed twice in the fail condition in src/modules/bluetooth/module-bluez5-device.c and src/modules/bluetooth/module-bluez5-device.c. Fixed in 1:8.0-0ubuntu3.14.	5.3	More Details
CVE-2020-3441	A vulnerability in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to view sensitive information from the meeting room lobby. This vulnerability is due to insufficient protection of sensitive participant information. An attacker could exploit this vulnerability by browsing the Webex roster. A successful exploit could allow the attacker to gather information about other Webex participants, such as email address and IP address, while waiting in the lobby.	5.3	More Details
CVE-2020-8278	Improper access control in Nextcloud Social app version 0.3.1 allowed to read posts of any user.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15928	In Ortus TestBox 2.4.0 through 4.1.0, unvalidated query string parameters to test-browser/index.cfm allow directory traversal.	5.3	More Details
CVE-2020-26235	In Rust time crate from version 0.2.7 and before version 0.2.23, unix-like operating systems may segfault due to dereferencing a dangling pointer in specific circumstances. This requires the user to set any environment variable in a different thread than the affected functions. The affected functions are time::UtcOffset::local_offset_at, time::UtcOffset::try_local_offset_at, time::UtcOffset::current_local_offset, time::UtcOffset::try_current_local_offset, time::OffsetDateTime::now_local and time::OffsetDateTime::try_now_local. Non-Unix targets are unaffected. This includes Windows and wasm. The issue was introduced in version 0.2.7 and fixed in version 0.2.23.	5.3	More Details
CVE-2020-20739	im_vips2dz in /libvips/libvips/deprecated/im_vips2dz.c in libvips before 8.8.2 has an uninitialized variable which may cause the leakage of remote server path or stack address.	5.3	More Details
CVE-2020-15247	October is a free, open-source, self-hosted CMS platform based on the Laravel PHP Framework. In October CMS from version 1.0.319 and before version 1.0.469, an authenticated backend user with the cms.manage_pages, cms.manage_layouts, or cms.manage_partials permissions who would normally not be permitted to provide PHP code to be executed by the CMS due to cms.enableSafeMode being enabled is able to write specific Twig code to escape the Twig sandbox and execute arbitrary PHP. This is not a problem for anyone that trusts their users with those permissions to normally write & manage PHP within the CMS by not having cms.enableSafeMode enabled, but would be a problem for anyone relying on cms.enableSafeMode to ensure that users with those permissions in production do not have access to write & execute arbitrary PHP. Issue has been patched in Build 469 (v1.0.469) and v1.1.0.	5.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26231	October is a free, open-source, self-hosted CMS platform based on the Laravel PHP Framework. A bypass of CVE-2020-15247 (fixed in 1.0.469 and 1.1.0) was discovered that has the same impact as CVE-2020-15247. An authenticated backend user with the cms.manage_pages, cms.manage_layouts, or cms.manage_partials permissions who would normally not be permitted to provide PHP code to be executed by the CMS due to cms.enableSafeMode being enabled is able to write specific Twig code to escape the Twig sandbox and execute arbitrary PHP. This is not a problem for anyone that trusts their users with those permissions to normally write & manage PHP within the CMS by not having cms.enableSafeMode enabled, but would be a problem for anyone relying on cms.enableSafeMode to ensure that users with those permissions in production do not have access to write & execute arbitrary PHP. Issue has been patched in Build 470 (v1.0.470) and v1.1.1.	5.2	More Details
CVE-2020-28974	A slab-out-of-bounds read in fbcon in the Linux kernel before 5.9.7 could be used by local attackers to read privileged information or potentially crash the kernel, aka CID-3c4e0dff2095. This occurs because KD_FONT_OP_COPY in drivers/tty/vt/vt.c can be used for manipulations such as font height.	5.0	More Details
CVE-2020-25725	In Xpdf 4.02, SplashOutputDev::endType3Char(GfxState *state) SplashOutputDev.cc:3079 is trying to use the freed `t3GlyphStack->cache`, which causes an `heap-use-after-free` problem. The codes of a previous fix for nested Type 3 characters wasn't correctly handling the case where a Type 3 char referred to another char in the same Type 3 font.	5.0	More Details
CVE-2020-26079	A vulnerability in the web UI of Cisco IoT Field Network Director (FND) could allow an authenticated, remote attacker to obtain hashes of user passwords on an affected device. The vulnerability is due to insufficient protection of user credentials. An attacker could exploit this vulnerability by logging in as an administrative user and crafting a call for user information. A successful exploit could allow the attacker to obtain hashes of user passwords on an affected device.	4.9	More Details
CVE-2019-14553	Improper authentication in EDK II may allow a privileged user to potentially enable information disclosure via network access.	4.9	More Details
CVE-2020-29002	includes/CologneBlueTemplate.php in the CologneBlue skin for MediaWiki through 1.35 allows XSS via a qbfind message supplied by an administrator.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24723	Cross Site Scripting (XSS) vulnerability in the Registration page of the admin panel in PHPGurukul User Registration & Login and User Management System With admin panel 2.1.	4.8	More Details
CVE-2020-4788	IBM Power9 (AIX 7.1, 7.2, and VIOS 3.1) processors could allow a local user to obtain sensitive information from the data in the L1 cache under extenuating circumstances. IBM X-Force ID: 189296.	4.7	More Details
CVE-2020-26215	Jupyter Notebook before version 6.1.5 has an Open redirect vulnerability. A maliciously crafted link to a notebook server could redirect the browser to a different website. All notebook servers are technically affected, however, these maliciously crafted links can only be reasonably made for known notebook server hosts. A link to your notebook server may appear safe, but ultimately redirect to a spoofed server on the public internet. The issue is patched in version 6.1.5.	4.4	More Details
CVE-2020-15437	The Linux kernel before version 5.8 is vulnerable to a NULL pointer dereference in drivers/tty/serial/8250/8250_core.c:serial8250_isa_init_ports() that allows local users to cause a denial of service by using the p->serial_in pointer which uninitialized.	4.4	More Details
CVE-2020-7568	A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists in Modicon M221 (all references, all versions) that could allow non sensitive information disclosure when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M221 controller.	4.3	More Details
CVE-2020-5947	In versions 16.0.0-16.0.0.1 and 15.1.0-15.1.1, on specific BIG-IP platforms, attackers may be able to obtain TCP sequence numbers from the BIG-IP system that can be reused in future connections with the same source and destination port and IP numbers. Only these platforms are affected: BIG-IP 2000 series (C112), BIG-IP 4000 series (C113), BIG-IP i2000 series (C117), BIG-IP i4000 series (C115), BIG-IP Virtual Edition (VE).	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28942	An issue exists in PrimeKey EJBCA before 7.4.3 when enrolling with EST while proxied through an RA over the Peers protocol. As a part of EJBCA's domain security model, the peer connector allows the restriction of client certificates (for the RA, not the end user) to a limited set of allowed CAs, thus restricting the accessibility of that RA to the rights it has within a specific role. While this works for other protocols such as CMP, it was found that the EJBCA enrollment over an EST implementation bypasses this check, allowing enrollment with a valid client certificate through any functioning and authenticated RA connected to the CA. NOTE: an attacker must already have a trusted client certificate and authorization to enroll against the targeted CA.	4.3	More Details
CVE-2020-28953	In BigBlueButton before 2.2.29, a user can vote more than once in a single poll.	4.3	More Details
CVE-2020-26077	A vulnerability in the access control functionality of Cisco IoT Field Network Director (FND) could allow an authenticated, remote attacker to view lists of users from different domains that are configured on an affected system. The vulnerability is due to improper access control. An attacker could exploit this vulnerability by sending an API request that alters the domain for a requested user list on an affected system. A successful exploit could allow the attacker to view lists of users from different domains on the affected system.	4.3	More Details
CVE-2020-26232	Jupyter Server before version 1.0.6 has an Open redirect vulnerability. A maliciously crafted link to a jupyter server could redirect the browser to a different website. All jupyter servers are technically affected, however, these maliciously crafted links can only be reasonably made for known jupyter server hosts. A link to your jupyter server may appear safe, but ultimately redirect to a spoofed server on the public internet.	4.1	More Details
CVE-2020-1778	When OTRS uses multiple backends for user authentication (with LDAP), agents are able to login even if the account is set to invalid. This issue affects OTRS; 8.0.9 and prior versions.	4.1	More Details
CVE-2020-26080	A vulnerability in the user management functionality of Cisco IoT Field Network Director (FND) could allow an authenticated, remote attacker to manage user information for users in different domains on an affected system. The vulnerability is due to improper domain access control. An attacker could exploit this vulnerability by manipulating JSON payloads to target different domains on an affected system. A successful exploit could allow the attacker to manage user information for users in different domains on an affected system.	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15248	October is a free, open-source, self-hosted CMS platform based on the Laravel PHP Framework. In October CMS from version 1.0.319 and before version 1.0.470, backend users with the default "Publisher" system role have access to create & manage users where they can choose which role the new user has. This means that a user with "Publisher" access has the ability to escalate their access to "Developer" access. Issue has been patched in Build 470 (v1.0.470) & v1.1.1.	4.0	More Details
CVE-2020-26229	TYPO3 is an open source PHP based web content management system. In TYPO3 from version 10.4.0, and before version 10.4.10, RSS widgets are susceptible to XML external entity processing. This vulnerability is reasonable, but is theoretical - it was not possible to actually reproduce the vulnerability with current PHP versions of supported and maintained system distributions. At least with libxml2 version 2.9, the processing of XML external entities is disabled per default - and cannot be exploited. Besides that, a valid backend user account is needed. Update to TYPO3 version 10.4.10 to fix the problem described.	3.7	More Details
CVE-2020-25688	A flaw was found in rhacm versions before 2.0.5 and before 2.1.0. Two internal service APIs were incorrectly provisioned using a test certificate from the source repository. This would result in all installations using the same certificates. If an attacker could observe network traffic internal to a cluster, they could use the private key to decode API requests that should be protected by TLS sessions, potentially obtaining information they would not otherwise be able to. These certificates are not used for service authentication, so no opportunity for impersonation or active MITM attacks were made possible.	3.5	More Details
CVE-2020-6879	Some ZTE devices have input verification vulnerabilities. The devices support configuring a static prefix through the web management page. The restriction of the front-end code can be bypassed by constructing a POST request message and sending the request to the creation of a static routing rule configuration interface. The WEB service backend fails to effectively verify the abnormal input. As a result, the attacker can successfully use the vulnerability to tamper parameter values. This affects: ZXHN Z500 V1.0.0.2B1.1000 and ZXHN F670L V1.1.10P1N2E. This is fixed in ZXHN Z500 V1.0.1.1B1.1000 and ZXHN F670L V1.1.10P2N2.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15249	October is a free, open-source, self-hosted CMS platform based on the Laravel PHP Framework. In October CMS from version 1.0.319 and before version 1.0.469, backend users with access to upload files were permitted to upload SVG files without any sanitization applied to the uploaded files. Since SVG files support being parsed as HTML by browsers, this means that they could theoretically upload Javascript that would be executed on a path under the website's domain (i.e. /storage/app/media/evil.svg), but they would have to convince their target to visit that location directly in the target's browser as the backend does not display SVGs inline anywhere, SVGs are only displayed as image resources in the backend and are thus unable to be executed. Issue has been patched in Build 469 (v1.0.469) & v1.1.0.	2.8	More Details
CVE-2020-13360	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details