SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 23 December 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-2020-25066	A heap-based buffer overflow in the Treck HTTP Server component before 6.0.1.68 allows remote attackers to cause a denial of service (crash/reset) or to possibly execute arbitrary code.	10.0	More Details
CVE-2020-12522	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26276	Fleet is an open source osquery manager. In Fleet before version 3.5.1, due to issues in Go's standard library XML parsing, a valid SAML response may be mutated by an attacker to modify the trusted document. This can result in allowing unverified logins from a SAML IdP. Users that configure Fleet with SSO login may be vulnerable to this issue. This issue is patched in 3.5.1. The fix was made using https://github.com/mattermost/xml-roundtrip-validator If upgrade to 3.5.1 is not possible, users should disable SSO authentication in Fleet.	10.0	More Details
CVE-2020-35489	The contact-form-7 (aka Contact Form 7) plugin before 5.3.2 for WordPress allows Unrestricted File Upload and remote code execution because a filename may contain special characters.	10.0	More Details
CVE-2020-35193	The official sonarqube docker images before alpine (Alpine specific) contain a blank password for a root user. System using the sonarqube docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-7203	A potential security vulnerability has been identified in HPE iLO Amplifier Pack server version 1.70. The vulnerability could be exploited to allow remote code execution.	9.8	More Details
CVE-2020-35551	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos chipsets) software. They allow attackers to conduct RPMB state-change attacks because an unauthorized RPMB write operation can be replayed, a related issue to CVE-2020-13799. The Samsung ID is SVE-2020-18100 (December 2020).	9.8	More Details
CVE-2020-25494	Xinuos (formerly SCO) Openserver v5 and v6 allows attackers to execute arbitrary commands via shell metacharacters in outputform or toclevels parameter to cgi-bin/printbook.	9.8	More Details
CVE-2020-20276	An unauthenticated stack-based buffer overflow vulnerability in common.c's handle_PORT in uftpd FTP server versions 2.10 and earlier can be abused to cause a crash and could potentially lead to remote code execution.	9.8	More Details
CVE-2020-20277	There are multiple unauthenticated directory traversal vulnerabilities in different FTP commands in uftpd FTP server versions 2.7 to 2.10 due to improper implementation of a chroot jail in common.c's compose_abspath function that can be abused to read or write to arbitrary files on the filesystem, leak process memory, or potentially lead to remote code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20298	Eval injection vulnerability in the parserCommom method in the ParserTemplate class in zzz_template.php in zzzphp 1.7.2 allows remote attackers to execute arbitrary commands.	9.8	More Details
CVE-2020-20300	SQL injection vulnerability in the wp_where function in WeiPHP 5.0.	9.8	More Details
CVE-2020-11974	In DolphinScheduler 1.2.0 and 1.2.1, with mysql connectorj a remote code execution vulnerability exists when choosing mysql as database.	9.8	More Details
CVE-2020-14224	A vulnerability in the MIME message handling of the HCL Notes v9 client could potentially be exploited by an unauthenticated attacker resulting in a stack buffer overflow. This could allow a remote attacker to crash the Notes application or inject code into the system which would execute with the privileges of the currently logged-in user.	9.8	More Details
CVE-2020-7200	A potential security vulnerability has been identified in HPE Systems Insight Manager (SIM) version 7.6. The vulnerability could be exploited to allow remote code execution.	9.8	More Details
CVE-2020-35590	LimitLoginAttempts.php in the limit-login-attempts-reloaded plugin before 2.17.4 for WordPress allows a bypass of (per IP address) rate limits because the X-Forwarded-For header can be forged. When the plugin is configured to accept an arbitrary header for the client source IP address, a malicious user is not limited to perform a brute force attack, because the client IP header accepts any arbitrary string. When randomizing the header input, the login count does not ever reach the maximum allowed retries.	9.8	More Details
CVE-2020-27780	A flaw was found in Linux-Pam in versions prior to 1.5.1 in the way it handle empty passwords for non-existing users. When the user doesn't exist PAM try to authenticate with root and in the case of an empty password it successfully authenticate.	9.8	More Details
CVE-2020-35276	EgavilanMedia ECM Address Book 1.0 is affected by SQL injection. An attacker can bypass the Admin Login panel through SQLi and get Admin access and add or remove any user.	9.8	More Details
CVE-2020-27846	A signature verification vulnerability exists in crewjam/saml. This flaw allows an attacker to bypass SAML Authentication. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4988	Loopback 8.0.0 contains a vulnerability that could allow an attacker to manipulate or pollute Javascript values and cause a denial of service or possibly execute code. IBM X-Force ID: 192706.	9.8	More Details
CVE-2020-21377	SQL injection vulnerability in yunyecms V2.0.1 via the selcart parameter.	9.8	More Details
CVE-2020-21378	SQL injection vulnerability in SeaCMS 10.1 (2020.02.08) via the id parameter in an edit action to admin_members_group.php.	9.8	More Details
CVE-2020-35604	An XXE attack can occur in Kronos WebTA 5.0.4 when SAML is used.	9.8	More Details
CVE-2020-35605	The Graphics Protocol feature in graphics.c in kitty before 0.19.3 allows remote attackers to execute arbitrary code because a filename containing special characters can be included in an error message.	9.8	More Details
CVE-2020-11717	An issue was discovered in Programi 014 31.01.2020. It has multiple SQL injection vulnerabilities.	9.8	More Details
CVE-2020-8995	Programi Bilanc Build 007 Release 014 31.01.2020 supplies a .exe file containing several hardcoded credentials to different servers that allow remote attackers to gain access to the complete infrastructure including the website, update server, and external issue tracking tools.	9.8	More Details
CVE-2020-24673	In S+ Operations and S+ Historian, a successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. This can lead to a loss of confidentiality and data integrity or even affect the product behavior and its availability.	9.8	More Details
CVE-2020-24675	In S+ Operations and S+ History, it is possible that an unauthenticated user could inject values to the Operations History server (or standalone S+ History server) and ultimately write values to the controlled process.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24683	The affected versions of S+ Operations (version 2.1 SP1 and earlier) used an approach for user authentication which relies on validation at the client node (client-side authentication). This is not as secure as having the server validate a client application before allowing a connection. Therefore, if the network communication or endpoints for these applications are not protected, unauthorized actors can bypass authentication and make unauthorized connections to the server application.	9.8	More Details
CVE-2020-35550	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), Q(10.0), and R(11.0) software. Attackers can bypass Factory Reset Protection (FRP) via StatusBar. The Samsung ID is SVE-2020-17888 (December 2020).	9.8	More Details
CVE-2020-13931	If Apache TomEE 8.0.0-M1 - 8.0.3, 7.1.0 - 7.1.3, 7.0.0-M1 - 7.0.8, 1.0.0 - 1.7.5 is configured to use the embedded ActiveMQ broker, and the broker config is misconfigured, a JMX port is opened on TCP port 1099, which does not include authentication. CVE-2020-11969 previously addressed the creation of the JMX management interface, however the incomplete fix did not cover this edge case.	9.8	More Details
CVE-2020-35468	The Appbase streams Docker image 2.1.2 contains a blank password for the root user. Systems deployed using affected versions of the streams container may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-8466	A command injection vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2, with the improved password hashing method enabled, could allow an unauthenticated attacker to execute certain commands by providing a manipulated password.	9.8	More Details
CVE-2020-35469	The Software AG Terracotta Server OSS Docker image 5.4.1 contains a blank password for the root user. Systems deployed using affected versions of the Terracotta Server OSS container may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-35476	A remote code execution vulnerability occurs in OpenTSDB through 2.4.0 via command injection in the yrange parameter. The yrange value is written to a gnuplot file in the /tmp directory. This file is then executed via the mygnuplot.sh shell script. (tsd/GraphHandler.java attempted to prevent command injections by blocking backticks but this is insufficient.)	9.8	More Details
CVE-2019-14480	AdRem NetCrunch 10.6.0.4587 has an Improper Session Handling vulnerability in the NetCrunch web client, which can lead to an authentication bypass or escalation of privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14482	AdRem NetCrunch 10.6.0.4587 has a hardcoded SSL private key vulnerability in the NetCrunch web client. The same hardcoded SSL private key is used across different customers' installations when no other SSL certificate is installed, which allows remote attackers to defeat cryptographic protection mechanisms by leveraging knowledge of this key from another installation.	9.8	More Details
CVE-2020-7781	This affects the package connection-tester before 0.2.1. The injection point is located in line 15 in index.js. The following PoC demonstrates the vulnerability:	9.8	More Details
CVE-2020-28929	Unrestricted access to the log downloader functionality in EPSON EPS TSE Server 8 (21.0.11) allows an unauthenticated attacker to remotely retrieve administrative hashed credentials via the maintenance/troubleshoot.php?download=1 URI.	9.8	More Details
CVE-2020-35185	The official ghost docker images before 2.16.1-alpine (Alpine specific) contain a blank password for a root user. System using the ghost docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-35187	The official telegraf docker images before 1.9.4-alpine (Alpine specific) contain a blank password for a root user. System using the telegraf docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-35189	The official kong docker images before 1.0.2-alpine (Alpine specific) contain a blank password for a root user. System using the kong docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-35184	The official composer docker images before 1.8.3 contain a blank password for a root user. System using the composer docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-35186	The official adminer docker images before 4.7.0-fastcgi contain a blank password for a root user. System using the adminer docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-35190	The official plone Docker images before version of 4.3.18-alpine (Alpine specific) contain a blank password for a root user. System using the plone docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35191	The official drupal docker images before 8.5.10-fpm-alpine (Alpine specific) contain a blank password for a root user. System using the drupal docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-35192	The official vault docker images before 0.11.6 contain a blank password for a root user. System using the vault docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-35195	The official haproxy docker images before 1.8.18-alpine (Alpine specific) contain a blank password for a root user. System using the haproxy docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-35196	The official rabbitmq docker images before 3.7.13-beta.1-management-alpine (Alpine specific) contain a blank password for a root user. System using the rabbitmq docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-35197	The official memcached docker images before 1.5.11-alpine (Alpine specific) contain a blank password for a root user. System using the memcached docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-25094	LogRhythm Platform Manager 7.4.9 allows Command Injection. To exploit this, an attacker can inject arbitrary program names and arguments into a WebSocket. These are forwarded to any remote server with a LogRhythm Smart Response agent installed. By default, the commands are run with LocalSystem privileges.	9.8	More Details
CVE-2020-25010	An arbitrary code execution vulnerability in Kyland KPS2204 6 Port Managed Din-Rail Programmable Serial Device Servers Software Version:R0002.P05 allows remote attackers to upload a malicious script file by constructing a POST type request and writing a payload in the request parameters as an instruction to write a file.	9.8	More Details
CVE-2020-25011	A sensitive information disclosure vulnerability in Kyland KPS2204 6 Port Managed Din-Rail Programmable Serial Device Servers Software Version:R0002.P05 allows remote attackers to get username and password by request /cgi-bin/webadminget.cgi script via the browser.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-22083	jsonpickle through 1.4.1 allows remote code execution during deserialization of a malicious payload through the decode() function. Note: It has been argued that this is expected and clearly documented behaviour. pickle is known to be capable of causing arbitrary code execution, and must not be used with un-trusted data	9.8	More Details
CVE-2020-35545	Time-based SQL injection exists in Spotweb 1.4.9 via the query string.	9.8	More Details
CVE-2020-8465	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an attacker to manipulate system updates using a combination of CSRF bypass (CVE-2020-8461) and authentication bypass (CVE-2020-8464) to execute code as user root.	9.8	More Details
CVE-2020-29583	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges.	9.8	More Details
CVE-2018-15632	Improper input validation in database creation logic in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier, allows remote attackers to initialize an empty database on which they can connect with default credentials.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-26280	OpenSlides is a free, Web-based presentation and assembly system for managing and projecting agenda, motions, and elections of assemblies. OpenSlides version 3.2, due to unsufficient user input validation and escaping, it is vulnerable to persistant cross-site scripting (XSS). In the web applications users can enter rich text in various places, e.g. for personal notes or in motions. These fields can be used to store arbitrary JavaScript Code that will be executed when other users read the respective text. An attacker could utilize this vulnerability be used to manipulate votes of other users, hijack the moderators session or simply disturb the meeting. The vulnerability was introduced with 6eae497abeab234418dfbd9d299e831eff86ed45 on 16.04.2020, which is first included in the 3.2 release. It has been patched in version 3.3 (in commit f3809fc8a97ee305d721662a75f788f9e9d21938, merged in master on 20.11.2020).	8.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35606	Arbitrary command execution can occur in Webmin through 1.962. Any user authorized for the Package Updates module can execute arbitrary commands with root privileges via vectors involving %0A and %0C. NOTE: this issue exists because of an incomplete fix for CVE-2019-12840.	8.8	More Details
CVE-2020-13513	A privilege escalation vulnerability exists in the WinRing0x64 Driver Privileged I/O Write IRPs functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause increased privileges. Using the IRP 0x9c40a0dc gives a low privilege user direct access to the OUT instruction that is completely unrestrained at an elevated privilege level. An attacker can send a malicious IRP to trigger this vulnerability.	8.8	More Details
CVE-2019-14479	AdRem NetCrunch 10.6.0.4587 allows Remote Code Execution. In the NetCrunch web client, a read-only administrator can execute arbitrary code on the server running the NetCrunch server software.	8.8	More Details
CVE-2020-35151	The Online Marriage Registration System 1.0 post parameter "searchdata" in the user/search.php request is vulnerable to Time Based Sql Injection.	8.8	More Details
CVE-2020-8461	A CSRF protection bypass vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an attacker to get a victim's browser to send a specifically encoded request without requiring a valid CSRF token.	8.8	More Details
CVE-2020-7201	A potential security vulnerability has been identified in the HPE StoreEver MSL2024 Tape Library and HPE StoreEver 1/8 G2 Tape Autoloaders. The vulnerability could be remotely exploited to allow Cross-site Request Forgery (CSRF).	8.8	More Details
CVE-2020-28931	Lack of an anti-CSRF token in the entire administrative interface in EPSON EPS TSE Server 8 (21.0.11) allows an unauthenticated attacker to force an administrator to execute external POST requests by visiting a malicious website.	8.8	More Details
CVE-2020-13519	A privilege escalation vulnerability exists in the WinRing0x64 Driver IRP 0x9c402088 functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause increased privileges. An attacker can send a malicious IRP to trigger this vulnerability.	8.8	More Details
CVE-2020-13515	A privilege escalation vulnerability exists in the WinRing0x64 Driver IRP 0x9c40a148 functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause an adversary to obtain elevated privileges. An attacker can send a malicious IRP to trigger this vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13514	A privilege escalation vulnerability exists in the WinRing0x64 Driver Privileged I/O Write IRPs functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause increased privileges. Using the IRP 0x9c40a0e0 gives a low privilege user direct access to the OUT instruction that is completely unrestrained at an elevated privilege level. An attacker can send a malicious IRP to trigger this vulnerability.	8.8	More Details
CVE-2020-13512	A privilege escalation vulnerability exists in the WinRing0x64 Driver Privileged I/O Write IRPs functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause increased privileges. Using the IRP 0x9c40a0d8 gives a low privilege user direct access to the OUT instruction that is completely unrestrained at an elevated privilege level. An attacker can send a malicious IRP to trigger this vulnerability.	8.8	More Details
CVE-2020-35626	An issue was discovered in the PushToWatch extension for MediaWiki through 1.35.1. The primary form did not implement an anti-CSRF token and therefore was completely vulnerable to CSRF attacks against onSkinAddFooterLinks in PushToWatch.php.	8.8	More Details
CVE-2020-27687	ThingsBoard before v3.2 is vulnerable to Host header injection in password-reset emails. This allows an attacker to send malicious links in password-reset emails to victims, pointing to an attacker-controlled server. Lack of validation of the Host header allows this to happen.	8.8	More Details
CVE-2020-26174	tangro Business Workflow before 1.18.1 requests a list of allowed filetypes from the server and restricts uploads to the filetypes contained in this list. However, this restriction is enforced in the browser (client-side) and can be circumvented. This allows an attacker to upload any file as an attachment to a workitem.	8.8	More Details
CVE-2020-25095	LogRhythm Platform Manager (PM) 7.4.9 allows CSRF. The Web interface is vulnerable to Cross-site WebSocket Hijacking (CSWH). If a logged-in PM user visits a malicious site in the same browser session, that site can perform a CSRF attack to create a WebSocket from the victim client to the vulnerable PM server. Once the socket is created, the malicious site can interact with the vulnerable web server in the context of the logged-in user. This can include WebSocket payloads that result in command execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25096	LogRhythm Platform Manager (PM) 7.4.9 has Incorrect Access Control. Users within LogRhythm can be delegated different roles and privileges, intended to limit what data and services they can interact with. However, no access control is enforced for WebSocket-based communication to the PM application server, which will forward requests to any configured back-end server, regardless of whether the user's access rights should permit this. As a result, even the most low-privileged user can interact with any back-end component that has a LogRhythm agent installed.	8.8	More Details
CVE-2020-27154	The chat window of Mitel BusinessCTI Enterprise (MBC-E) Client for Windows before 6.4.11 and 7.x before 7.0.3 could allow an attacker to gain access to user information by sending arbitrary code, due to improper input validation. A successful exploit could allow an attacker to view the user information and application data.	8.8	More Details
CVE-2020-7838	A arbitrary code execution vulnerability exists in the way that the Stove client improperly validates input value. An attacker could execute arbitrary code when the user access to crafted web page. This issue affects: Smilegate STOVE Client 0.0.4.72.	8.8	More Details
CVE-2020-14232	A vulnerability in the input parameter handling of HCL Notes v9 could potentially be exploited by an authenticated attacker resulting in a stack buffer overflow. This could allow the attacker to crash the program or inject code into the system which would execute with the privileges of the currently logged in user.	8.8	More Details
CVE-2020-12519	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use this vulnerability i.e. to open a reverse shell with root privileges.	8.8	More Details
CVE-2020-35625	An issue was discovered in the Widgets extension for MediaWiki through 1.35.1. Any user with the ability to edit pages within the Widgets namespace could call any static function within any class (defined within PHP or MediaWiki) via a crafted HTML comment, related to a Smarty template. For example, a person in the Widget Editors group could use \MediaWiki\Shell\Shell::command within a comment.	8.8	More Details
CVE-2020-12517	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an authenticated low privileged user could embed malicious Javascript code to gain admin rights when the admin user visits the vulnerable website (local privilege escalation).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-11781	Improper input validation in portal component in Odoo Community 12.0 and earlier and Odoo Enterprise 12.0 and earlier, allows remote attackers to trick victims into modifying their account via crafted links, leading to privilege escalation.	8.8	More Details
CVE-2020-25622	An issue was discovered in SolarWinds N-Central 12.3.0.670. The AdvancedScripts HTTP endpoint allows CSRF.	8.8	More Details
CVE-2020-25618	An issue was discovered in SolarWinds N-Central 12.3.0.670. The sudo configuration has incorrect access control because the nable web user account is effectively able to run arbitrary OS commands as root (i.e., the use of root privileges is not limited to specific programs listed in the sudoers file).	8.8	More Details
CVE-2020-14231	A vulnerability in the input parameter handling of HCL Client Application Access v9 could potentially be exploited by an authenticated attacker resulting in a stack buffer overflow. This could allow the attacker to crash the program or inject code into the system which would execute with the privileges of the currently logged in user.	8.8	More Details
CVE-2020-29396	A sandboxing issue in Odoo Community 11.0 through 13.0 and Odoo Enterprise 11.0 through 13.0, when running with Python 3.6 or later, allows remote authenticated users to execute arbitrary code, leading to privilege escalation.	8.8	More Details
CVE-2020-24579	An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. An unauthenticated attacker could bypass authentication to access authenticated pages and functionality.	8.8	More Details
CVE-2020-13547	A type confusion vulnerability exists in the JavaScript engine of Foxit Software's Foxit PDF Reader, version 10.1.0.37527. A specially crafted PDF document can trigger an improper use of an object, resulting in memory corruption and arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability.	8.8	More Details
CVE-2020-24674	In S+ Operations and S+ Historian, not all client commands correctly check user permission as expected. Authenticated but Unauthorized remote users could execute a Denial-of-Service (DoS) attack, execute arbitrary code, or obtain more privilege than intended on the machines.	8.8	More Details
CVE-2020-24677	Vulnerabilities in the S+ Operations and S+ Historian web applications can lead to a possible code execution and privilege escalation, redirect the user somewhere else or download unwanted data.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13570	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 10.1.0.37527. A specially crafted PDF document can trigger the reuse of previously free memory which can lead to arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability.	8.8	More Details
CVE-2020-13560	A use after free vulnerability exists in the JavaScript engine of Foxit Software's Foxit PDF Reader, version 10.1.0.37527. A specially crafted PDF document can trigger reuse of previously free memory which can lead to arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability.	8.8	More Details
CVE-2020-13557	A use after free vulnerability exists in the JavaScript engine of Foxit Software's Foxit PDF Reader, version 10.1.0.37527. A specially crafted PDF document can trigger reuse of previously free memory which can lead to arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability.	8.8	More Details
CVE-2019-14483	AdRem NetCrunch 10.6.0.4587 allows Credentials Disclosure. Every user can read the BSD, Linux, MacOS and Solaris private keys, private keys' passwords, and root passwords stored in the credential manager. Every administrator can read the ESX and Windows passwords stored in the credential manager.	8.8	More Details
CVE-2020-24678	An authenticated user might execute malicious code under the user context and take control of the system. S+ Operations or S+ Historian database is affected by multiple vulnerabilities such as the possibility to allow remote authenticated users to gain high privileges.	8.8	More Details
CVE-2020-25617	An issue was discovered in SolarWinds N-Central 12.3.0.670. The AdvancedScripts HTTP endpoint allows Relative Path Traversal by an authenticated user of the N-Central Administration Console (NAC), leading to execution of OS commands as root.	8.8	More Details
CVE-2020-25621	An issue was discovered in SolarWinds N-Central 12.3.0.670. The local database does not require authentication: security is only based on ability to access a network interface. The database has keys and passwords.	8.4	More Details
CVE-2020-5803	Relative Path Traversal in Marvell QConvergeConsole GUI 5.5.0.74 allows a remote, authenticated attacker to delete arbitrary files on disk as SYSTEM or root.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27640	The Bluetooth handset of Mitel MiVoice 6940 and 6930 MiNet phones with firmware before 1.5.3 could allow an unauthenticated attacker within Bluetooth range to pair a rogue Bluetooth device when a phone handset loses connection, due to an improper pairing mechanism. A successful exploit could allow an attacker to eavesdrop on conversations.	8.1	More Details
CVE-2020-28052	An issue was discovered in Legion of the Bouncy Castle BC Java 1.65 and 1.66. The OpenBSDBCrypt.checkPassword utility method compared incorrect data when checking the password, allowing incorrect passwords to indicate they were matching with previously hashed ones that were different.	8.1	More Details
CVE-2020-35490	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.dbcp2.datasources.PerUserPoolDataSource.	8.1	More Details
CVE-2020-35491	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.dbcp2.datasources.SharedPoolDataSource.	8.1	More Details
CVE-2020-27639	The Bluetooth handset of Mitel MiVoice 6873i, 6930, and 6940 SIP phones with firmware before 5.1.0.SP6 could allow an unauthenticated attacker within Bluetooth range to pair a rogue Bluetooth device when a phone handset loses connection, due to an improper pairing mechanism. A successful exploit could allow an attacker to eavesdrop on conversations.	8.1	More Details
CVE-2020-24581	An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. It contains an execute_cmd.cgi feature (that is not reachable via the web user interface) that lets an authenticated user execute Operating System commands.	8.0	More Details
CVE-2020-35273	EgavilanMedia User Registration & Login System with Admin Panel 1.0 is affected by Cross Site Request Forgery (CSRF) to remotely gain privileges in the User Profile panel. An attacker can update any user's account.	8.0	More Details
CVE-2020-35554	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10 software. There is a WebView SSL error-handler vulnerability. The LG ID is LVE-SMP-200026 (December 2020).	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35608	A code execution vulnerability exists in the normal world's signed code execution functionality of Microsoft Azure Sphere 20.07. A specially crafted AF_PACKET socket can cause a process to create an executable memory mapping with controllable content. An attacker can execute a shellcode that uses the PACKET_MMAP functionality to trigger this vulnerability.	7.8	More Details
CVE-2020-25106	Nanosystems SupRemo 4.1.3.2348 allows attackers to obtain LocalSystem access because File Manager can be used to rename Supremo.exe and then upload a Trojan horse with the Supremo.exe filename.	7.8	More Details
CVE-2020-24676	In Symphony Plus Operations and Symphony Plus Historian, some services can be vulnerable to privilege escalation attacks. An unprivileged (but authenticated) user could execute arbitrary code and result in privilege escalation, depending on the user that the service runs as.	7.8	More Details
CVE-2020-25620	An issue was discovered in SolarWinds N-Central 12.3.0.670. Hard-coded Credentials exist by default for local user accounts named support@n-able.com and nableadmin@n-able.com. These allow logins to the N-Central Administrative Console (NAC) and/or the regular web interface.	7.8	More Details
CVE-2020-13535	A privilege escalation vulnerability exists in Kepware LinkMaster 3.0.94.0. In its default configuration, an attacker can globally overwrite service configuration to execute arbitrary code with NT SYSTEM privileges.	7.8	More Details
CVE-2020-15294	Compiler Optimization Removal or Modification of Security-critical Code vulnerability in IntPeParseUnwindData() results in multiple dereferences to the same pointer. If the pointer is located in memory-mapped from the guest space, this may cause a race-condition where the generated code would dereference the same address twice, thus obtaining different values, which may lead to arbitrary code execution. This issue affects: Bitdefender Hypervisor Introspection versions prior to 1.132.2.	7.8	More Details
CVE-2020-35555	An issue was discovered on LG mobile devices with Android OS 10 software. When a dual-screen configuration is supported, the device does not lock upon disconnection of a call with the cover closed. The LG ID is LVE-SMP-200027 (December 2020).	7.8	More Details
CVE-2020-17526	Incorrect Session Validation in Apache Airflow Webserver versions prior to 1.10.14 with default config allows a malicious airflow user on site A where they log in normally, to access unauthorized Airflow Webserver on Site B through the session from Site A. This does not affect users who have changed the default value for `[webserver] secret_key` config.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26284	Hugo is a fast and Flexible Static Site Generator built in Go. Hugo depends on Go's `os/exec` for certain features, e.g. for rendering of Pandoc documents if these binaries are found in the system `%PATH%` on Windows. In Hugo before version 0.79.1, if a malicious file with the same name (`exe` or `bat`) is found in the current working directory at the time of running `hugo`, the malicious command will be invoked instead of the system one. Windows users who run `hugo` inside untrusted Hugo sites are affected. Users should upgrade to Hugo v0.79.1. Other than avoiding untrusted Hugo sites, there is no workaround.	7.7	More Details
CVE-2020-26258	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.15, a Server-Side Forgery Request vulnerability can be activated when unmarshalling. The vulnerability may allow a remote attacker to request data from internal resources that are not publicly available only by manipulating the processed input stream. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.15. The reported vulnerability does not exist if running Java 15 or higher. No user is affected who followed the recommendation to setup XStream's Security Framework with a whitelist! Anyone relying on XStream's default blacklist can immediately switch to a whilelist for the allowed types to avoid the vulnerability. Users of XStream 1.4.14 or below who still want to use XStream default blacklist can use a workaround described in more detailed in the referenced advisories.	7.7	More Details
CVE-2020-35573	srs2.c in PostSRSd before 1.10 allows remote attackers to cause a denial of service (CPU consumption) via a long timestamp tag in an SRS address.	7.5	More Details
CVE-2020-29652	A nil pointer dereference in the golang.org/x/crypto/ssh component through v0.0.0-20201203163018-be400aefbc4c for Go allows remote attackers to cause a denial of service against SSH servers.	7.5	More Details
CVE-2020-35475	In MediaWiki before 1.35.1, the messages userrights-expiry-current and userrights-expiry-none can contain raw HTML. XSS can happen when a user visits Special:UserRights but does not have rights to change all userrights, and the table on the left side has unchangeable groups in it. (The right column with the changeable groups is not affected and is escaped correctly.)	7.5	More Details
CVE-2020-35553	An issue was discovered on Samsung mobile devices with Q(10.0) and R(11.0) (Qualcomm SM8250 chipsets) software. They allows attackers to cause a denial of service (unlock failure) by triggering a power-shortage incident that causes a false-positive attack detection. The Samsung ID is SVE-2020-19678 (December 2020).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20299	WeiPHP 5.0 does not properly restrict access to pages, related to using POST.	7.5	More Details
CVE-2020-35579	tindy2013 subconverter 0.6.4 has a /sub?target=%TARGET%&url=%URL%&config=%CONFIG% API endpoint that accepts an arbitrary %URL% value and launches a GET request for it, but does not consider that the external request target may indirectly redirect back to this original /sub endpoint. Thus, a request loop and a denial of service may occur.	7.5	More Details
CVE-2020-35133	irfanView 4.56 contains an error processing parsing files of type .pcx. Which leads to out-of-bounds writing at i_view32+0xdb60.	7.5	More Details
CVE-2020-26263	tlslite-ng is an open source python library that implements SSL and TLS cryptographic protocols. In tlslite-ng before versions 0.7.6 and 0.8.0-alpha39, the code that performs decryption and padding check in RSA PKCS#1 v1.5 decryption is data dependant. In particular, the code has multiple ways in which it leaks information about the decrypted ciphertext. It aborts as soon as the plaintext doesn't start with 0x00, 0x02. All TLS servers that enable RSA key exchange as well as applications that use the RSA decryption API directly are vulnerable. This is patched in versions 0.7.6 and 0.8.0-alpha39. Note: the patches depend on Python processing the individual bytes in side-channel free manner, this is known to not the case (see reference). As such, users that require side-channel resistance are recommended to use different TLS implementations, as stated in the security policy of tlslite-ng.	7.5	More Details
CVE-2020-27254	Emerson Rosemount X-STREAM Gas AnalyzerX-STREAM enhanced XEGP, XEGK, XEFD, XEXF – all revisions, The affected products are vulnerable to improper authentication for accessing log and backup data, which could allow an attacker with a specially crafted URL to obtain access to sensitive information.	7.5	More Details
CVE-2020-4870	IBM MQ 9.2 CD and LTS are vulnerable to a denial of service attack caused by an error processing connecting applications. IBM X-Force ID: 190833.	7.5	More Details
CVE-2020-5808	In certain scenarios in Tenable.sc prior to 5.17.0, a scanner could potentially be used outside the user's defined scan zone without a particular zone being specified within the Automatic Distribution configuration.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6881	ZTE E8810/E8820/E8822 series routers have an MQTT DoS vulnerability, which is caused by the failure of the device to verify the validity of abnormal messages. A remote attacker could connect to the MQTT server and send an MQTT exception message to the specified device, which will cause the device to deny service. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13>	7.5	More Details
CVE-2020-6882	ZTE E8810/E8820/E8822 series routers have an information leak vulnerability, which is caused by hard-coded MQTT service access credentials on the device. The remote attacker could use this credential to connect to the MQTT server, so as to obtain information about other devices by sending specific topics. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13>	7.5	More Details
CVE-2020-7837	An issue was discovered in ML Report Program. There is a stack-based buffer overflow in function sub_41EAF0 at MLReportDeamon.exe. The function will call vsprintf without checking the length of strings in parameters given by attacker. And it finally leads to a stack-based buffer overflow via access to crafted web page. This issue affects: Infraware ML Report 2.19.312.0000.	7.5	More Details
CVE-2018-7580	Philips Hue is vulnerable to a Denial of Service attack. Sending a SYN flood on port tcp/80 will freeze Philips Hue's hub and it will stop responding. The "hub" will stop operating and be frozen until the flood stops. During the flood, the user won't be able to turn on/off the lights, and all of the hub's functionality will be unresponsive. The cloud service also won't work with the hub.	7.5	More Details
CVE-2020-29596	MiniWeb HTTP server 0.8.19 allows remote attackers to cause a denial of service (daemon crash) via a long name for the first parameter in a POST request.	7.5	More Details
CVE-2020-35623	An issue was discovered in the CasAuth extension for MediaWiki through 1.35.1. Due to improper username validation, it allowed user impersonation with trivial manipulations of certain characters within a given username. An ordinary user may be able to login as a "bureaucrat user" who has a similar username, as demonstrated by usernames that differ only in (1) bidirectional override symbols or (2) blank space.	7.5	More Details
CVE-2020-5360	Dell BSAFE Micro Edition Suite, versions prior to 4.5, are vulnerable to a Buffer Under-Read Vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability resulting in undefined behaviour, or a crash of the affected systems.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8463	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an attacker to bypass a global authorization check for anonymous users by manipulating request paths.	7.5	More Details
CVE-2020-8464	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an attacker to send requests that appear to come from the localhost which could expose the product's admin interface to users who would not normally have access.	7.5	More Details
CVE-2020-24679	A S+ Operations and S+ Historian service is subject to a DoS by special crafted messages. An attacker might use this flaw to make it crash or even execute arbitrary code on the machine where the service is hosted.	7.5	More Details
CVE-2020-5682	Improper input validation in GROWI versions prior to v4.2.3 (v4.2 Series), GROWI versions prior to v4.1.12 (v4.1 Series), and GROWI v3 series and earlier GROWI versions prior to v4.2.3 (v4.2 Series), GROWI versions prior to v4.1.12 (v4.1 Series), and GROWI v3 series and earlier allows remote attackers to cause a denial of service via unspecified vectors.	7.5	More Details
CVE-2020-5683	Directory traversal vulnerability in GROWI versions prior to v4.2.3 (v4.2 Series), GROWI versions prior to v4.1.12 (v4.1 Series), and GROWI v3 series and earlier GROWI versions prior to v4.2.3 (v4.2 Series), GROWI versions prior to v4.1.12 (v4.1 Series), and GROWI v3 series and earlier allows remote attackers to alter the data by uploading a specially crafted file.	7.5	More Details
CVE-2020-29361	An issue was discovered in p11-kit 0.21.1 through 0.23.21. Multiple integer overflows have been discovered in the array allocations in the p11-kit library and the p11-kit list command, where overflow checks are missing before calling realloc or calloc.	7.5	More Details
CVE-2020-24580	An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. Lack of authentication functionality allows an attacker to assign a static IP address that was once used by a valid user.	7.5	More Details
CVE-2020-29363	An issue was discovered in p11-kit 0.23.6 through 0.23.21. A heap-based buffer overflow has been discovered in the RPC protocol used by p11-kit server/remote commands and the client library. When the remote entity supplies a serialized byte array in a CK_ATTRIBUTE, the receiving entity may not allocate sufficient length for the buffer to store the deserialized value.	7.5	More Details
CVE-2020-14254	TLS-RSA cipher suites are not disabled in HCL BigFix Inventory up to v10.0.2. If TLS 2.0 and secure ciphers are not enabled then an attacker can passively record traffic and later decrypt it.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27199	The Magic Home Pro application 1.5.1 for Android allows Authentication Bypass. The security control that the application currently has in place is a simple Username and Password authentication function. Using enumeration, an attacker is able to forge a User specific token without the need for correct password to gain access to the mobile application as that victim user.	7.5	More Details
CVE-2020-28458	All versions of package datatables.net are vulnerable to Prototype Pollution due to an incomplete fix for https://snyk.io/vuln/SNYK-JS-DATATABLESNET-598806.	7.3	More Details
CVE-2020-27337	An issue was discovered in Treck IPv6 before 6.0.1.68. Improper Input Validation in the IPv6 component allows an unauthenticated remote attacker to cause an Out of Bounds Write, and possibly a Denial of Service via network access.	7.3	More Details
CVE-2020-25608	The SAS portal of Mitel MiCollab before 9.2 could allow an attacker to access user credentials due to improper input validation, aka SQL Injection.	7.2	More Details
CVE-2020-29607	A file upload restriction bypass vulnerability in Pluck CMS before 4.7.13 allows an admin privileged user to gain access in the host through the "manage files" functionality, which may result in remote code execution.	7.2	More Details
CVE-2020-27781	User credentials can be manipulated and stolen by Native CephFS consumers of OpenStack Manila, resulting in potential privilege escalation. An Open Stack Manila user can request access to a share to an arbitrary cephx user, including existing users. The access key is retrieved via the interface drivers. Then, all users of the requesting OpenStack project can view the access key. This enables the attacker to target any resource that the user has access to. This can be done to even "admin" users, compromising the ceph administrator. This flaw affects Ceph versions prior to 14.2.16, 15.x prior to 15.2.8, and 16.x prior to 16.2.0.	7.1	More Details
CVE-2020-28641	In Malwarebytes Free 4.1.0.56, a symbolic link may be used delete an arbitrary file on the system by exploiting the local quarantine system.	7.1	More Details
CVE-2020-24680	In S+ Operations and S+ Historian, the passwords of internal users (not Windows Users) are encrypted but improperly stored in a database.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26281	async-h1 is an asynchronous HTTP/1.1 parser for Rust (crates.io). There is a request smuggling vulnerability in async-h1 before version 2.3.0. This vulnerability affects any webserver that uses async-h1 behind a reverse proxy, including all such Tide applications. If the server does not read the body of a request which is longer than some buffer length, async-h1 will attempt to read a subsequent request from the body content starting at that offset into the body. One way to exploit this vulnerability would be for an adversary to craft a request such that the body contains a request that would not be noticed by a reverse proxy, allowing it to forge forwarded/x-forwarded headers. If an application trusted the authenticity of these headers, it could be misled by the smuggled request. Another potential concern with this vulnerability is that if a reverse proxy is sending multiple http clients' requests along the same keep-alive connection, it would be possible for the smuggled request to specify a long content and capture another user's request in its body. This content could be captured in a post request to an endpoint that allows the content to be subsequently retrieved by the adversary. This has been addressed in async-h1 2.3.0 and previous versions have been yanked.	6.8	More Details
CVE-2020-26259	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.15, is vulnerable to an Arbitrary File Deletion on the local host when unmarshalling. The vulnerability may allow a remote attacker to delete arbitrary know files on the host as log as the executing process has sufficient rights only by manipulating the processed input stream. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.15. The reported vulnerability does not exist running Java 15 or higher. No user is affected, who followed the recommendation to setup XStream's Security Framework with a whitelist! Anyone relying on XStream's default blacklist can immediately switch to a whilelist for the allowed types to avoid the vulnerability. Users of XStream 1.4.14 or below who still want to use XStream default blacklist can use a workaround described in more detailed in the referenced advisories.	6.8	More Details
CVE-2020-25860	The install.c module in the Pengutronix RAUC update client prior to version 1.5 has a Time-of-Check Time-of-Use vulnerability, where signature verification on an update file takes place before the file is reopened for installation. An attacker who can modify the update file just before it is reopened can install arbitrary code on the device.	6.6	More Details
CVE-2020-4904	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35123	In Zimbra Collaboration Suite Network Edition versions < 9.0.0 P10 and 8.8.15 P17, there exists an XXE vulnerability in the saml consumer store extension, which is vulnerable to XXE attacks. This has been fixed in Zimbra Collaboration Suite Network edition 9.0.0 Patch 10 and 8.8.15 Patch 17.	6.5	More Details
CVE-2020-13510	An information disclosure vulnerability exists in the WinRing0x64 Driver Privileged I/O Read IRPs functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) using the IRP 0x9c4060d0 gives a low privilege user direct access to the IN instruction that is completely unrestrained at an elevated privilege level. An attacker can send a malicious IRP to trigger this vulnerability.	6.5	More Details
CVE-2019-11783	Improper access control in mail module (channel partners) in Odoo Community 14.0 and earlier and Odoo Enterprise 14.0 and earlier, allows remote authenticated users to subscribe to arbitrary mail channels uninvited.	6.5	More Details
CVE-2019-11784	Improper access control in mail module (notifications) in Odoo Community 14.0 and earlier and Odoo Enterprise 14.0 and earlier, allows remote authenticated users to obtain access to arbitrary messages in conversations they were not a party to.	6.5	More Details
CVE-2020-13511	An information disclosure vulnerability exists in the WinRing0x64 Driver Privileged I/O Read IRPs functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) using the IRP 0x9c4060d4 gives a low privilege user direct access to the IN instruction that is completely unrestrained at an elevated privilege level. An attacker can send a malicious IRP to trigger this vulnerability.	6.5	More Details
CVE-2020-26175	In tangro Business Workflow before 1.18.1, an attacker can manipulate the value of PERSON in requests to /api/profile in order to change profile information of other users.	6.5	More Details
CVE-2018-15645	Improper access control in message routing in Odoo Community 12.0 and earlier and Odoo Enterprise 12.0 and earlier allows remote authenticated users to create arbitrary records via crafted payloads, which may allow privilege escalation.	6.5	More Details
CVE-2020-17520	In the Pulsar manager 0.1.0 version, malicious users will be able to bypass pulsar-manager's admin, permission verification mechanism by constructing special URLs, thereby accessing any HTTP API.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24578	An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. It has a misconfigured FTP service that allows a malicious network user to access system folders and download sensitive files (such as the password hash file).	6.5	More Details
CVE-2019-14476	AdRem NetCrunch 10.6.0.4587 has a Server-Side Request Forgery (SSRF) vulnerability in the NetCrunch server. Every user can trick the server into performing SMB requests to other systems.	6.5	More Details
CVE-2020-4764	IBM Planning Analytics 2.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 188898.	6.5	More Details
CVE-2019-16959	SolarWinds Web Help Desk 12.7.0 allows CSV Injection, also known as Formula Injection, via a file attached to a ticket.	6.5	More Details
CVE-2020-3999	VMware ESXi (7.0 prior to ESXi70U1c-17325551), VMware Workstation (16.x prior to 16.0 and 15.x prior to 15.5.7), VMware Fusion (12.x prior to 12.0 and 11.x prior to 11.5.7) and VMware Cloud Foundation contain a denial of service vulnerability due to improper input validation in GuestInfo. A malicious actor with normal user privilege access to a virtual machine can crash the virtual machine's vmx process leading to a denial of service condition.	6.5	More Details
CVE-2020-13516	An information disclosure vulnerability exists in the WinRing0x64 Driver IRP 0x9c406144 functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause the disclosure of sensitive information. An attacker can send a malicious IRP to trigger this vulnerability.	6.5	More Details
CVE-2020-35497	A flaw was found in ovirt-engine 4.4.3 and earlier allowing an authenticated user to read other users' personal information, including name, email and public SSH key.	6.5	More Details
CVE-2020-12521	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS a specially crafted LLDP packet may lead to a high system load in the PROFINET stack. An attacker can cause failure of system services or a complete reboot.	6.5	More Details
CVE-2020-14225	HCL iNotes is susceptible to a Tabnabbing vulnerability caused by improper sanitization of message content. A remote unauthenticated attacker could use this vulnerability to trick the end user into entering sensitive information such as credentials, e.g. as part of a phishing attack.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29436	Sonatype Nexus Repository Manager 3.x before 3.29.0 allows a user with admin privileges to configure the system to gain access to content outside of NXRM via an XXE vulnerability. Fixed in version 3.29.0.	6.5	More Details
CVE-2020-13518	An information disclosure vulnerability exists in the WinRing0x64 Driver IRP 0x9c402084 functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause the disclosure of sensitive information. An attacker can send a malicious IRP to trigger this vulnerability.	6.5	More Details
CVE-2020-13509	An information disclosure vulnerability exists in the WinRing0x64 Driver Privileged I/O Read IRPs functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) Using the IRP 0x9c4060cc gives a low privilege user direct access to the IN instruction that is completely unrestrained at an elevated privilege level. An attacker can send a malicious IRP to trigger this vulnerability and this access could allow for information leakage of sensitive data.	6.5	More Details
CVE-2019-11782	Improper access control in Odoo Community 14.0 and earlier and Odoo Enterprise 14.0 and earlier, allows remote authenticated users with access to contact management to modify user accounts, leading to privilege escalation.	6.5	More Details
CVE-2020-4757	IBM FileNet Content Manager and IBM Content Navigator 3.0.CD 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: 188600.	6.4	More Details
CVE-2020-26274	In systeminformation (npm package) before version 4.31.1 there is a command injection vulnerability. The problem was fixed in version 4.31.1 with a shell string sanitation fix.	6.4	More Details
CVE-2020-25606	The AWV component of Mitel MiCollab before 9.2 could allow an attacker to view system information by sending arbitrary code due to improper input validation, aka XSS.	6.1	More Details
CVE-2020-35622	An issue was discovered in the GlobalUsage extension for MediaWiki through 1.35.1. SpecialGlobalUsage.php calls WikiMap::makeForeignLink unsafely. The $page variable within the formatItem function was not being properly escaped, allowing for XSS under certain conditions.	6.1	More Details
CVE-2020-26049	Nifty-PM CPE 2.3 is affected by stored HTML injection. The impact is remote arbitrary code execution.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26277	DBdeployer is a tool that deploys MySQL database servers easily. In DBdeployer before version 1.58.2, users unpacking a tarball may use a maliciously packaged tarball that contains symlinks to files external to the target. In such scenario, an attacker could induce dbdeployer to write into a system file, thus altering the computer defenses. For the attack to succeed, the following factors need to contribute: 1) The user is logged in as root. While dbdeployer is usable as root, it was designed to run as unprivileged user. 2) The user has taken a tarball from a non secure source, without testing the checksum. When the tarball is retrieved through dbdeployer, the checksum is compared before attempting to unpack. This has been fixed in version 1.58.2.	6.1	More Details
CVE-2020-26275	The Jupyter Server provides the backend (i.e. the core services, APIs, and REST endpoints) for Jupyter web applications like Jupyter notebook, JupyterLab, and Voila. In Jupyter Server before version 1.1.1, an open redirect vulnerability could cause the jupyter server to redirect the browser to a different malicious website. All jupyter servers running without a base_url prefix 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. This same vulnerability was patched in upstream notebook v5.7.8. This is fixed in jupyter_server 1.1.1. If upgrade is not available, a workaround can be to run your server on a url prefix: "jupyter server --ServerApp.base_url=/jupyter/".	6.1	More Details
CVE-2020-14271	HCL iNotes v9, v10 and v11 is susceptible to a Stored Cross-Site Scripting (XSS) vulnerability due to improper handling of message content. An unauthenticated remote attacker could exploit this vulnerability using specially-crafted markup to execute script in a victim's web browser within the security context of the hosting Web site and/or steal the victim's cookie-based authentication credentials.	6.1	More Details
CVE-2020-4080	HCL Verse v10 and v11 is susceptible to a Stored Cross-Site Scripting (XSS) vulnerability due to improper handling of message content. An unauthenticated remote attacker could exploit this vulnerability using specially-crafted markup to execute script in a victim's web browser within the security context of the hosting Web site and/or steal the victim's cookie-based authentication credentials.	6.1	More Details
CVE-2020-4657	IBM Sterling B2B Integrator 5.2.0.0 through 6.0.3.2 Standard Edition is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 186094.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15293	Memory corruption in IntLixCrashDumpDmesg, IntLixTaskFetchCmdLine, IntLixFileReadDentry and IntLixFileGetPath due to insufficient guest-data input validation may lead to denial of service conditions.	6.1	More Details
CVE-2020-27340	The online help portal of Mitel MiCollab before 9.2 could allow an attacker to redirect a user to an unauthorized website by executing malicious script due to insufficient access control.	6.1	More Details
CVE-2020-4658	IBM Sterling File Gateway 2.2.0.0 through 6.0.3.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 186095.	6.1	More Details
CVE-2020-20142	Cross Site Scripting (XSS) vulnerability in the "To Remote CSV" component under "Open" Menu in Flexmonster Pivot Table & Charts 2.7.17.	6.1	More Details
CVE-2020-35474	In MediaWiki before 1.35.1, the combination of Html::rawElement and Message::text leads to XSS because the definition of MediaWiki:recentchanges-legend-watchlistexpiry can be changed onwiki so that the output is raw HTML.	6.1	More Details
CVE-2020-35478	MediaWiki before 1.35.1 allows XSS via BlockLogFormatter.php. MediaWiki:blanknamespace potentially can be output as raw HTML with SCRIPT tags via LogFormatter::makePageLink(). This affects MediaWiki 1.33.0 and later.	6.1	More Details
CVE-2020-35479	MediaWiki before 1.35.1 allows XSS via BlockLogFormatter.php. Language::translateBlockExpiry itself does not escape in all code paths. For example, the return of Language::userTimeAndDate is is always unsafe for HTML in a month value. This affects MediaWiki 1.12.0 and later.	6.1	More Details
CVE-2020-20138	Cross Site Scripting (XSS) vulnerability in the Showtime2 Slideshow module in CMS Made Simple (CMSMS) 2.2.4.	6.1	More Details
CVE-2020-20139	Cross Site Scripting (XSS) vulnerability in the Remote JSON component Under the Connect menu in Flexmonster Pivot Table & Charts 2.7.17.	6.1	More Details
CVE-2020-20140	Cross Site Scripting (XSS) vulnerability in Remote Report component under the Open menu in Flexmonster Pivot Table & Charts 2.7.17.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20141	Cross Site Scripting (XSS) vulnerability in the To OLAP (XMLA) component Under the Connect menu in Flexmonster Pivot Table & Charts 2.7.17.	6.1	More Details
CVE-2020-25611	The AWV portal of Mitel MiCollab before 9.2 could allow an attacker to gain access to conference information by sending arbitrary code due to improper input validation, aka XSS. Successful exploitation could allow an attacker to view user conference information.	6.1	More Details
CVE-2020-26198	Dell EMC iDRAC9 versions prior to 4.32.10.00 and 4.40.00.00 contain a reflected cross-site scripting vulnerability in the iDRAC9 web application. A remote attacker could potentially exploit this vulnerability to run malicious HTML or JavaScript in a victim's browser by tricking a victim in to following a specially crafted link.	6.1	More Details
CVE-2020-25495	A reflected Cross-site scripting (XSS) vulnerability in Xinuo (formerly SCO) Openserver version 5 and 6 allows remote attackers to inject arbitrary web script or HTML tag via the parameter 'section'.	6.1	More Details
CVE-2020-25901	Host Header Injection in Spiceworks 7.5.7.0 allowing the attacker to render arbitrary links that point to a malicious website with poisoned Host header webpages.	6.1	More Details
CVE-2018-15634	Cross-site scripting (XSS) issue in attachment management in Odoo Community 14.0 and earlier and Odoo Enterprise 14.0 and earlier, allows remote attackers to inject arbitrary web script in the browser of a victim via a crafted link.	6.1	More Details
CVE-2020-4840	IBM Security Secret Server 10.6 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 190044.	6.1	More Details
CVE-2018-15633	Cross-site scripting (XSS) issue in "document" module in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier, allows remote attackers to inject arbitrary web script in the browser of a victim via crafted attachment filenames.	6.1	More Details
CVE-2020-4905	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 could allow an remote attacker to obtain sensitive information, caused by a man in the middle attack. By SSL striping, an attacker could exploit this vulnerability to obtain sensitive information.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27338	An issue was discovered in Treck IPv6 before 6.0.1.68. Improper Input Validation in the DHCPv6 client component allows an unauthenticated remote attacker to cause an Out of Bounds Read, and possibly a Denial of Service via adjacent network access.	5.9	More Details
CVE-2020-4841	IBM Security Secret Server 10.6 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: 190045.	5.9	More Details
CVE-2020-5359	Dell BSAFE Micro Edition Suite, versions prior to 4.5, are vulnerable to an Unchecked Return Value Vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability to modify and corrupt the encrypted data.	5.8	More Details
CVE-2020-28460	This affects the package multi-ini before 2.1.2. It is possible to pollute an object's prototype by specifying the constructor.proto object as part of an array. This is a bypass of CVE-2020-28448.	5.6	More Details
CVE-2020-28448	This affects the package multi-ini before 2.1.1. It is possible to pollute an object's prototype by specifying the proto object as part of an array.	5.6	More Details
CVE-2019-14477	AdRem NetCrunch 10.6.0.4587 has Improper Credential Storage since the internal user database is readable by low-privileged users and passwords in the database are weakly encoded or encrypted.	5.5	More Details
CVE-2020-13517	An information disclosure vulnerability exists in the WinRing0x64 Driver IRP 0x9c406104 functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause the disclosure of sensitive information. An attacker can send a malicious IRP to trigger this vulnerability.	5.5	More Details
CVE-2020-35609	A denial-of-service vulnerability exists in the asynchronous ioctl functionality of Microsoft Azure Sphere 20.05. A sequence of specially crafted ioctl calls can cause a denial of service. An attacker can write shellcode to trigger this vulnerability.	5.5	More Details
CVE-2020-12518	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use the knowledge gained by reading the insufficiently protected sensitive information to plan further attacks.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15292	Lack of validation on data read from guest memory in IntPeGetDirectory, IntPeParseUnwindData, IntLogExceptionRecord, IntKsymExpandSymbol and IntLixTaskDumpTree may lead to out-of-bounds read or it could cause DoS due to integer-overflor (IntPeGetDirectory), TOCTOU (IntPeParseUnwindData) or insufficient validations.	5.5	More Details
CVE-2020-35549	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Any application may establish itself as the default dialer, without user interaction. The Samsung ID is SVE-2020-19172 (December 2020).	5.5	More Details
CVE-2020-35548	An issue was discovered in Finder on Samsung mobile devices with Q(10.0) software. A call to a non-existent provider allows attackers to cause a denial of service. The Samsung ID is SVE-2020-18629 (December 2020).	5.5	More Details
CVE-2020-4794	IBM Automation Workstream Services 19.0.3, 20.0.1, 20.0.2, IBM Business Automation Workflow 18.0, 19.0, and 20.0 and IBM Business Process Manager 8.6 could allow an authenticated user to obtain sensitive information or cuase a denial of service due to iimproper authorization checking. IBM X-Force ID: 189445.	5.4	More Details
CVE-2020-35275	Coastercms v5.8.18 is affected by cross-site Scripting (XSS). A user can steal a cookie and make the user redirect to any malicious website because it is trigged on the main home page of the product/application.	5.4	More Details
CVE-2020-20285	There is a XSS in the user login page in zzcms 2019. Users can inject js code by the referer header via user/login.php	5.4	More Details
CVE-2020-4555	IBM Financial Transaction Manager 3.0.6 and 3.1.0 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 183328.	5.4	More Details
CVE-2020-25609	The NuPoint Messenger Portal of Mitel MiCollab before 9.2 could allow an authenticated attacker to execute arbitrary scripts due to insufficient input validation, aka XSS. A successful exploit could allow an attacker to view and modify user data.	5.4	More Details
CVE-2020-28930	A Cross-Site Scripting (XSS) issue in the 'update user' and 'delete user' functionalities in settings/users.php in EPSON EPS TSE Server 8 (21.0.11) allows an authenticated attacker to inject a JavaScript payload in the user management page that is executed by an administrator.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14478	AdRem NetCrunch 10.6.0.4587 has a stored Cross-Site Scripting (XSS) vulnerability in the NetCrunch web client. The user's input data is not properly encoded when being echoed back to the user. This data can be interpreted as executable code by the browser and allows an attacker to execute JavaScript code in the context of the user's browser if the victim opens or searches for a node whose "Display Name" contains an XSS payload.	5.4	More Details
CVE-2020-35589	The limit-login-attempts-reloaded plugin before 2.17.4 for WordPress allows wp-admin/options-general.php?page=limit-login-attempts&tab= XSS. A malicious user can cause an administrator user to supply dangerous content to the vulnerable page, which is then reflected back to the user and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to victims.	5.4	More Details
CVE-2018-15638	Cross-site scripting (XSS) issue in mail module in Odoo Community 13.0 and earlier and Odoo Enterprise 13.0 and earlier, allows remote attackers to inject arbitrary web script in the browser of a victim via crafted channel names.	5.4	More Details
CVE-2018-15641	Cross-site scripting (XSS) issue in web module in Odoo Community 11.0 through 14.0 and Odoo Enterprise 11.0 through 14.0, allows remote authenticated internal users to inject arbitrary web script in the browser of a victim via crafted calendar event attributes.	5.4	More Details
CVE-2019-14481	AdRem NetCrunch 10.6.0.4587 has a Cross-Site Request Forgery (CSRF) vulnerability in the NetCrunch web client. Successful exploitation requires a logged-in user to open a malicious page and leads to account takeover.	5.4	More Details
CVE-2019-16957	SolarWinds Web Help Desk 12.7.0 allows XSS via the First Name field of a User Account.	5.4	More Details
CVE-2020-12523	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource	5.4	More Details
CVE-2019-16955	SolarWinds Web Help Desk 12.7.0 allows XSS via an uploaded SVG document in a request.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4845	IBM Security Key Lifecycle Manager 3.0.1 and 4.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 190289.	5.4	More Details
CVE-2020-14270	HCL Domino v9, v10, v11 is susceptible to an Information Disclosure vulnerability in XPages due to improper error handling of user input. An unauthenticated attacker could exploit this vulnerability to obtain information about the XPages software running on the Domino server.	5.3	More Details
CVE-2020-35552	An issue was discovered in the GPS daemon on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (non-Qualcomm chipsets) software. Attackers can obtain sensitive location information because the configuration file is incorrect. The Samsung ID is SVE-2020-18678 (December 2020).	5.3	More Details
CVE-2020-14248	BigFix Inventory up to v10.0.2 does not set the secure flag for the session cookie in an https session, which can cause the cookie to be sent in http requests and make it easier for remote attackers to capture this cookie.	5.3	More Details
CVE-2020-35480	An issue was discovered in MediaWiki before 1.35.1. Missing users (accounts that don't exist) and hidden users (accounts that have been explicitly hidden due to being abusive, or similar) that the viewer cannot see are handled differently, exposing sensitive information about the hidden status to unprivileged viewers. This exists on various code paths.	5.3	More Details
CVE-2020-35477	MediaWiki before 1.35.1 blocks legitimate attempts to hide log entries in some situations. If one sets MediaWiki:Mainpage to Special:MyLanguage/Main Page, visits a log entry on Special:Log, and toggles the "Change visibility of selected log entries" checkbox (or a tags checkbox) next to it, there is a redirection to the main page's action=historysubmit (instead of the desired behavior in which a revision-deletion form appears).	5.3	More Details
CVE-2020-25610	The AWV component of Mitel MiCollab before 9.2 could allow an attacker to gain access to a web conference due to insufficient access control for conference codes.	5.3	More Details
CVE-2020-29362	An issue was discovered in p11-kit 0.21.1 through 0.23.21. A heap-based buffer over-read has been discovered in the RPC protocol used by thep11-kit server/remote commands and the client library. When the remote entity supplies a byte array through a serialized PKCS#11 function call, the receiving entity may allow the reading of up to 4 bytes of memory past the heap allocation.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26178	In tangro Business Workflow before 1.18.1, knowing an attachment ID, it is possible to download workitem attachments without being authenticated.	5.3	More Details
CVE-2020-35177	HashiCorp Vault and Vault Enterprise 1.4.1 and newer allowed the enumeration of users via the LDAP auth method. Fixed in 1.5.6 and 1.6.1.	5.3	More Details
CVE-2020-13528	An information disclosure vulnerability exists in the Web Manager and telnet CLI functionality of Lantronix XPort EDGE 3.0.0.0R11, 3.1.0.0R9, 3.4.0.0R12 and 4.2.0.0R7. A specially crafted HTTP request can cause information disclosure. An attacker can sniff the network to trigger this vulnerability.	5.3	More Details
CVE-2020-35624	An issue was discovered in the SecurePoll extension for MediaWiki through 1.35.1. The non-admin vote list contains a full vote timestamp, which may provide unintended clues about how a voting process unfolded.	5.3	More Details
CVE-2020-35453	HashiCorp Vault Enterprise's Sentinel EGP policy feature incorrectly allowed requests to be processed in parent and sibling namespaces. Fixed in 1.5.6 and 1.6.1.	5.3	More Details
CVE-2020-4908	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 returns the product version and release information on the login dialog. This information could be used in further attacks against the system.	5.3	More Details
CVE-2020-4907	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.	5.3	More Details
CVE-2020-26273	osquery is a SQL powered operating system instrumentation, monitoring, and analytics framework. In osquery before version 4.6.0, by using sqlite's ATTACH verb, someone with administrative access to osquery can cause reads and writes to arbitrary sqlite databases on disk. This _does_ allow arbitrary files to be created, but they will be sqlite databases. It does not appear to allow existing non-sqlite files to be overwritten. This has been patched in osquery 4.6.0. There are several mitigating factors and possible workarounds. In some deployments, the people with access to these interfaces may be considered administrators. In some deployments, configuration is managed by a central tool. This tool can filter for the `ATTACH` keyword. osquery can be run as non-root user. Because this also limits the desired access levels, this requires deployment specific testing and configuration.	5.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4842	IBM Security Secret Server 10.6 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 190046.	4.9	More Details
CVE-2020-25612	The NuPoint Messenger of Mitel MiCollab before 9.2 could allow an attacker with escalated privilege to access user files due to insufficient access control. Successful exploit could potentially allow an attacker to gain access to sensitive information.	4.9	More Details
CVE-2020-35274	DotCMS Add Template with admin panel 20.11 is affected by cross-site Scripting (XSS) to gain remote privileges. An attacker could compromise the security of a website or web application through a stored XSS attack and stealing cookies using XSS.	4.8	More Details
CVE-2020-8462	A cross-site scripting (XSS) vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an attacker to tamper with the web interface of the product.	4.8	More Details
CVE-2020-27010	A cross-site scripting (XSS) vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an attacker to tamper with the web interface of the product in a manner separate from the similar CVE-2020-8462.	4.8	More Details
CVE-2020-14874	Vulnerability in the Oracle Cloud Infrastructure Identity and Access Management product of Oracle Cloud Services. Easily exploitable vulnerability allows high privileged attacker with network access to compromise Oracle Cloud Infrastructure Identity and Access Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Cloud Infrastructure Identity and Access Management accessible data as well as unauthorized read access to a subset of Oracle Cloud Infrastructure Identity and Access Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Cloud Infrastructure Identity and Access Management.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26251	Open Zaak is a modern, open-source data- and services-layer to enable zaakgericht werken, a Dutch approach to case management. In Open Zaak before version 1.3.3 the Cross-Origin-Resource-Sharing policy in Open Zaak is currently wide open - every client is allowed. This allows evil.com to run scripts that perform AJAX calls to known Open Zaak installations, and the browser will not block these. This was intended to only apply to development machines running on localhost/127.0.0.1. Open Zaak 1.3.3 disables CORS by default, while it can be opted-in through environment variables. The vulnerability does not actually seem exploitable because: a) The session cookie has a `Same-Site: Lax` policy which prevents it from being sent along in Cross-Origin requests. b) All pages that give access to (production) data are login-protected c) `Access-Control-Allow-Credentials` is set to `false` d) CSRF checks probably block the remote origin, since they're not explicitly added to the trusted allowlist.	4.7	More Details
CVE-2020-13527	An authentication bypass vulnerability exists in the Web Manager functionality of Lantronix XPort EDGE 3.0.0.0R11, 3.1.0.0R9, 3.4.0.0R12 and 4.2.0.0R7. A specially crafted HTTP request can cause increased privileges. An attacker can send an HTTP request to trigger this vulnerability.	4.5	More Details
CVE-2020-25619	An issue was discovered in SolarWinds N-Central 12.3.0.670. The SSH component does not restrict the Communication Channel to Intended Endpoints. An attacker can leverage an SSH feature (port forwarding with a temporary key pair) to access network services on the 127.0.0.1 interface, even though this feature was only intended for user-to-agent communication.	4.4	More Details
CVE-2020-4843	IBM Security Secret Server 10.6 stores potentially sensitive information in config files that could be read by an authenticated user. IBM X-Force ID: 190048.	4.3	More Details
CVE-2020-29447	Affected versions of Atlassian Crucible allow remote attackers to impact the application's availability via a Denial of Service (DoS) vulnerability in the file upload request feature of code reviews. The affected versions are before version 4.7.4, and from version 4.8.0 before 4.8.5.	4.3	More Details
CVE-2020-26171	In tangro Business Workflow before 1.18.1, the documentId of attachment uploads to /api/document/attachments/upload can be manipulated. By doing this, users can add attachments to workitems that do not belong to them.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26176	An issue was discovered in tangro Business Workflow before 1.18.1. No (or broken) access control checks exist on the /api/document/<DocumentID>/attachments API endpoint. Knowing a document ID, an attacker can list all the attachments of a workitem, including their respective IDs. This allows the attacker to gather valid attachment IDs for workitems that do not belong to them.	4.3	More Details
CVE-2019-11786	Improper access control in Odoo Community 13.0 and earlier and Odoo Enterprise 13.0 and earlier, allows remote authenticated users to modify translated terms, which may lead to arbitrary content modification on translatable elements.	4.3	More Details
CVE-2019-11785	Improper access control in mail module (followers) in Odoo Community 13.0 and earlier and Odoo Enterprise 13.0 and earlier, allows remote authenticated users to obtain access to messages posted on business records there were not given access to, and subscribe to receive future messages.	4.3	More Details
CVE-2020-26177	In tangro Business Workflow before 1.18.1, a user's profile contains some items that are greyed out and thus are not intended to be edited by regular users. However, this restriction is only applied client-side. Manipulating any of the greyed-out values in requests to /api/profile is not prohibited server-side.	4.3	More Details
CVE-2020-26172	Every login in tangro Business Workflow before 1.18.1 generates the same JWT token, which allows an attacker to reuse the token when a session is active. The JWT token does not contain an expiration timestamp.	4.2	More Details
CVE-2020-26422	Buffer overflow in QUIC dissector in Wireshark 3.4.0 to 3.4.1 allows denial of service via packet injection or crafted capture file	3.7	More Details
CVE-2020-27336	An issue was discovered in Treck IPv6 before 6.0.1.68. Improper input validation in the IPv6 component when handling a packet sent by an unauthenticated remote attacker could result in an out-of-bounds read of up to three bytes via network access.	3.7	More Details
CVE-2020-4008	The installer of the macOS Sensor for VMware Carbon Black Cloud (prior to 3.5.1) handles certain files in an insecure way. A malicious actor who has local access to the endpoint on which a macOS sensor is going to be installed, may overwrite a limited number of files with output from the sensor installation.	3.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24693	The Ignite portal in Mitel MiContact Center Business before 9.3.0.0 could allow a local attacker to view system information due to insufficient output sanitization.	3.3	More Details
CVE-2020-4906	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 allows web pages to be stored locally which can be read by another user on the system.	3.3	More Details
CVE-2020-26173	An incorrect access control implementation in Tangro Business Workflow before 1.18.1 allows an attacker to download documents (PDF) by providing a valid document ID and token. No further authentication is required.	3.1	More Details
CVE-2020-4846	IBM Security Key Lifecycle Manager 3.0.1 and 4.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 190290.	2.7	More Details
CVE-2020-35194	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-5021. Reason: This candidate is a reservation duplicate of CVE-2019-5021. Notes: All CVE users should reference CVE-2019-5021 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-35188	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-5021. Reason: This candidate is a reservation duplicate of CVE-2019-5021. Notes: All CVE users should reference CVE-2019-5021 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usag	N/A	More Details