SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 18 March 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-2020-1953	Apache Commons Configuration uses a third-party library to parse YAML files which by default allows the instantiation of classes if the YAML includes special statements. Apache Commons Configuration versions 2.2, 2.3, 2.4, 2.5, 2.6 did not change the default settings of this library. So if a YAML file was loaded from an untrusted source, it could therefore load and execute code out of the control of the host application.	10.0	More Details
CVE-2020-0796	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.	10.0	More Details
CVE-2020-10376	Technicolor TC7337NET 08.89.17.23.03 devices allow remote attackers to discover passwords by sniffing the network for an "Authorization: Basic" HTTP header.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7603	closure-compiler-stream through 0.1.15 allows execution of arbitrary commands. The argument "options" of the exports function in "index.js" can be controlled by users without any sanitization.	9.8	More Details
CVE-2020-5542	Buffer error vulnerability in TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier allows remote attackers to stop the network functions or execute malware via a specially crafted packet.	9.8	More Details
CVE-2020-7607	gulp-styledocco through 0.0.3 allows execution of arbitrary commands. The argument 'options' of the exports function in 'index.js' can be controlled by users without any sanitization.	9.8	More Details
CVE-2020-7606	docker-compose-remote-api through 0.1.4 allows execution of arbitrary commands. Within 'index.js' of the package, the function 'exec(serviceName, cmd, fnStdout, fnStderr, fnExit)' uses the variable 'serviceName' which can be controlled by users without any sanitization.	9.8	More Details
CVE-2020-7605	gulp-tape through 1.0.0 allows execution of arbitrary commands. It is possible to inject arbitrary commands as part of 'gulp-tape' options.	9.8	More Details
CVE-2020-7604	pulverizr through 0.7.0 allows execution of arbitrary commands. Within "lib/job.js", the variable "filename" can be controlled by the attacker. This function uses the variable "filename" to construct the argument of the exec call without any sanitization. In order to successfully exploit this vulnerability, an attacker will need to create a new file with the same name as the attack command.	9.8	More Details
CVE-2020-7602	node-prompt-here through 1.0.1 allows execution of arbitrary commands. The "runCommand()" is called by "getDevices()" function in file "linux/manager.js", which is required by the "index. process.env.NM_CLI" in the file "linux/manager.js". This function is used to construct the argument of function "execSync()", which can be controlled by users without any sanitization.	9.8	More Details
CVE-2020-5544	Null Pointer Dereference vulnerability in TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier allows remote attackers to stop the network functions or execute malware via a specially crafted packet.	9.8	More Details
CVE-2020-7601	gulp-scss-lint through 1.0.0 allows execution of arbitrary commands. It is possible to inject arbitrary commands to the "exec" function located in "src/command.js" via the provided options.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0086	In readCString of Parcel.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to arbitrary code execution if IntSan were not enabled, which it is by default. No additional execution privileges are required. User interaction is not needed for exploitation. Product: Android Versions: Android-10 Android ID: A-131859347	9.8	More Details
CVE-2020-10574	An issue was discovered in Janus through 0.9.1. janus.c tries to use a string that doesn't actually exist during a "query_logger" Admin API request, because of a typo in the JSON validation.	9.8	More Details
CVE-2020-10571	An issue was discovered in psd-tools before 1.9.4. The Cython implementation of RLE decoding did not check for malicious data.	9.8	More Details
CVE-2020-10567	An issue was discovered in Responsive Filemanager through 9.14.0. In the ajax_calls.php file in the save_img action in the name parameter, there is no validation of what kind of extension is sent. This makes it possible to execute PHP code if a legitimate JPEG image contains this code in the EXIF data, and the .php extension is used in the name parameter. (A potential fast patch is to disable the save_img action in the config file.)	9.8	More Details
CVE-2020-10564	An issue was discovered in the File Upload plugin before 4.13.0 for WordPress. A directory traversal can lead to remote code execution by uploading a crafted txt file into the lib directory, because of a wfu_include_lib call.	9.8	More Details
CVE-2020-10563	An issue was discovered in DEVOME GRR before 3.4.1c. frmcontactlist.php mishandles a SQL query.	9.8	More Details
CVE-2020-5543	TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier does not properly manage sessions, which allows remote attackers to stop the network functions or execute malware via a specially crafted packet.	9.8	More Details
CVE-2020-5545	TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier allows remote attackers to bypass access restriction and to stop the network functions or execute malware via a specially crafted packet.	9.8	More Details
CVE-2019-14299	Ricoh SP C250DN 1.05 devices have an Authentication Method Vulnerable to Brute Force Attacks. Some Ricoh printers did not implement account lockout. Therefore, it was possible to obtain the local account credentials by brute force.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8784	SuiteCRM 7.10.x versions prior to 7.10.23 and 7.11.x versions prior to 7.11.11 allow SQL Injection (issue 2 of 4).	9.8	More Details
CVE-2020-10119	cPanel before 84.0.20 allows a demo account to achieve remote code execution via a cpsrvd rsync shell (SEC-544).	9.8	More Details
CVE-2019-20498	cPanel before 82.0.18 allows WebDAV authentication bypass because the connection-sharing logic is incorrect (SEC-534).	9.8	More Details
CVE-2020-10380	RMySQL through 0.10.19 allows SQL Injection.	9.8	More Details
CVE-2020-9347	Zoho ManageEngine Password Manager Pro through 10.x has a CSV Excel Macro Injection vulnerability via a crafted name that is mishandled by the Export Passwords feature. NOTE: the vendor disputes the significance of this report because they expect CSV risk mitigation to be provided by an external application, and do not plan to add CSV constraints to their own products	9.8	More Details
CVE-2020-8786	SuiteCRM 7.10.x versions prior to 7.10.23 and 7.11.x versions prior to 7.11.11 allow SQL Injection (issue 4 of 4).	9.8	More Details
CVE-2020-8785	SuiteCRM 7.10.x versions prior to 7.10.23 and 7.11.x versions prior to 7.11.11 allow SQL Injection (issue 3 of 4).	9.8	More Details
CVE-2020-8783	SuiteCRM 7.10.x versions prior to 7.10.23 and 7.11.x versions prior to 7.11.11 allow SQL Injection (issue 1 of 4).	9.8	More Details
CVE-2020-5547	Resource Management Errors vulnerability in TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier allows remote attackers to stop the network functions or execute malware via a specially crafted packet.	9.8	More Details
CVE-2019-19212	Dolibarr ERP/CRM 3.0 through 10.0.3 allows XSS via the qty parameter to product/fournisseurs.php (product price screen).	9.8	More Details
CVE-2020-5847	Unraid through 6.8.0 allows Remote Code Execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6990	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic key utilized to help protect the account password is hard coded into the RSLogix 500 binary file. An attacker could identify cryptographic keys and use it for further cryptographic attacks that could ultimately lead to a remote attacker gaining unauthorized access to the controller.	9.8	More Details
CVE-2020-10243	An issue was discovered in Joomla! before 3.9.16. The lack of type casting of a variable in a SQL statement leads to a SQL injection vulnerability in the Featured Articles frontend menutype.	9.8	More Details
CVE-2020-10230	CentOS-WebPanel.com (aka CWP) CentOS Web Panel (for CentOS 6 and 7) allows SQL Injection via the /cwp_{SESSION_HASH}/admin/loader_ajax.php term parameter.	9.8	More Details
CVE-2019-19208	Codiad Web IDE through 2.8.4 allows PHP Code injection.	9.8	More Details
CVE-2020-5203	In Fat-Free Framework 3.7.1, attackers can achieve arbitrary code execution if developers choose to pass user controlled input (e.g., $_REQUEST, $_GET, or $_POST) to the framework's Clear method.	9.8	More Details
CVE-2019-14310	Ricoh SP C250DN 1.05 devices allow denial of service (issue 2 of 3). Unauthenticated crafted packets to the IPP service will cause a vulnerable device to crash. A memory corruption has been identified in the way of how the embedded device parsed the IPP packets	9.8	More Details
CVE-2019-13202	Some Kyocera printers (such as the ECOSYS M5526cdw 2R7_2000.001.701) were affected by a buffer overflow vulnerability in the okhtmlfile and failhtmlfile parameters of several functionalities of the web application that would allow an unauthenticated attacker to perform a Denial of Service attack, crashing the device, or potentially execute arbitrary code on the device.	9.8	More Details
CVE-2020-10541	Zoho ManageEngine OpManager before 12.4.179 allows remote code execution via a specially crafted Mail Server Settings v1 API request. This was fixed in 12.5.108.	9.8	More Details
CVE-2019-9095	An issue was discovered on Moxa MGate MB3170 and MB3270 devices before 4.1, MB3280 and MB3480 devices before 3.1, MB3660 devices before 2.3, and MB3180 devices before 2.1. An attacker may be able to intercept weakly encrypted passwords and gain administrative access.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-9096	An issue was discovered on Moxa MGate MB3170 and MB3270 devices before 4.1, MB3280 and MB3480 devices before 3.1, MB3660 devices before 2.3, and MB3180 devices before 2.1. Insufficient password requirements for the MGate web application may allow an attacker to gain access by brute-forcing account passwords.	9.8	More Details
CVE-2019-9099	An issue was discovered on Moxa MGate MB3170 and MB3270 devices before 4.1, MB3280 and MB3480 devices before 3.1, MB3660 devices before 2.3, and MB3180 devices before 2.1. A Buffer overflow in the built-in web server allows remote attackers to initiate DoS, and probably to execute arbitrary code (issue 1 of 2).	9.8	More Details
CVE-2020-10181	goform/formEMR30 in Sumavision Enhanced Multimedia Router (EMR) 3.0.4.27 allows creation of arbitrary users with elevated privileges (administrator) on a device, as demonstrated by a setString=new_user<*1*>administrator<*1*>123456 request.	9.8	More Details
CVE-2020-8540	An XML external entity (XXE) vulnerability in Zoho ManageEngine Desktop Central before the 07-Mar-2020 update allows remote unauthenticated users to read arbitrary files or conduct server-side request forgery (SSRF) attacks via a crafted DTD in an XML request.	9.8	More Details
CVE-2020-1947	In Apache ShardingSphere(incubator) 4.0.0-RC3 and 4.0.0, the ShardingSphere's web console uses the SnakeYAML library for parsing YAML inputs to load datasource configuration. SnakeYAML allows to unmarshal data to a Java type By using the YAML tag. Unmarshalling untrusted data can lead to security flaws of RCE.	9.8	More Details
CVE-2019-10807	Blamer versions prior to 1.0.1 allows execution of arbitrary commands. It is possible to inject arbitrary commands as part of the arguments provided to blamer.	9.8	More Details
CVE-2020-10108	In Twisted Web through 19.10.0, there was an HTTP request splitting vulnerability. When presented with two content-length headers, it ignored the first header. When the second content-length value was set to zero, the request body was interpreted as a pipelined request.	9.8	More Details
CVE-2020-10109	In Twisted Web through 19.10.0, there was an HTTP request splitting vulnerability. When presented with a content-length and a chunked encoding header, the content-length took precedence and the remainder of the request body was interpreted as a pipelined request.	9.8	More Details
CVE-2020-0690	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0902	An elevation of privilege vulnerability exists in Service Fabric File Store Service under certain conditions, aka 'Service Fabric Elevation of Privilege'.	9.8	More Details
CVE-2019-11343	Torpedo Query before 2.5.3 mishandles the LIKE operator in ConditionBuilder.java, LikeCondition.java, and NotLikeCondition.java.	9.8	More Details
CVE-2019-13201	Some Kyocera printers (such as the ECOSYS M5526cdw 2R7_2000.001.701) were affected by a buffer overflow vulnerability in the LPD service. This would allow an unauthenticated attacker to cause a Denial of Service (DoS) in the LPD service and potentially execute arbitrary code on the device.	9.8	More Details
CVE-2020-10534	In the GlobalBlocking extension before 2020-03-10 for MediaWiki through 1.34.0, an issue related to IP range evaluation resulted in blocked users re-gaining escalated privileges. This is related to the case in which an IP address is contained in two ranges, one of which is locally disabled.	9.8	More Details
CVE-2019-17658	An unquoted service path vulnerability in the FortiClient FortiTray component of FortiClientWindows v6.2.2 and prior allow an attacker to gain elevated privileges via the FortiClientConsole executable service path.	9.8	More Details
CVE-2019-12182	Directory Traversal in Safescan Timemoto and TA-8000 series version 1.0 allows unauthenticated remote attackers to execute code via the administrative API.	9.8	More Details
CVE-2019-13165	Some Xerox printers (such as the Phaser 3320 V53.006.16.000) were affected by a buffer overflow vulnerability in the request parser of the IPP service. This would allow an unauthenticated attacker to cause a Denial of Service (DoS) and potentially execute arbitrary code on the device.	9.8	More Details
CVE-2019-13197	Some Kyocera printers (such as the ECOSYS M5526cdw 2R7_2000.001.701) were affected by a buffer overflow vulnerability in the URI paths of the web application that would allow an unauthenticated attacker to perform a Denial of Service attack, crashing the device, or potentially execute arbitrary code on the device.	9.8	More Details
CVE-2019-13192	Some Brother printers (such as the HL-L8360CDW v1.20) were affected by a heap buffer overflow vulnerability as the IPP service did not parse attribute names properly. This would allow an attacker to execute arbitrary code on the device.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-13172	Some Xerox printers (such as the Phaser 3320 V53.006.16.000) were affected by a buffer overflow vulnerability in the Authentication Cookie of the web application that would allow an attacker to execute arbitrary code on the device.	9.8	More Details
CVE-2019-13171	Some Xerox printers (such as the Phaser 3320 V53.006.16.000) were affected by one or more stack-based buffer overflow vulnerabilities in the Google Cloud Print implementation that would allow an unauthenticated attacker to execute arbitrary code on the device. This was caused by an insecure handling of the register parameters, because the size used within a memcpy() function, which copied the action value into a local variable, was not checked properly.	9.8	More Details
CVE-2019-13169	Some Xerox printers (such as the Phaser 3320 V53.006.16.000) were affected by a buffer overflow vulnerability in the Content-Type HTTP Header of the web application that would allow an attacker to execute arbitrary code on the device.	9.8	More Details
CVE-2019-13168	Some Xerox printers (such as the Phaser 3320 V53.006.16.000) were affected by a buffer overflow vulnerability in the attributes parser of the IPP service. This would allow an unauthenticated attacker to cause a Denial of Service (DoS) and potentially execute arbitrary code on the device.	9.8	More Details
CVE-2020-10121	cPanel before 84.0.20 allows a demo account to achieve code execution via PassengerApps APIs (SEC-546).	9.8	More Details
CVE-2020-10077	GitLab EE 3.0 through 12.8.1 allows SSRF. An internal investigation revealed that a particular deprecated service was creating a server side request forgery risk.	9.8	More Details
CVE-2020-10074	GitLab 10.1 through 12.8.1 has Incorrect Access Control. A scenario was discovered in which a GitLab account could be taken over through an expired link.	9.8	More Details
CVE-2019-13394	The Voo branded NETGEAR CG3700b custom firmware V2.02.03 uses HTTP Basic Authentication over cleartext HTTP.	9.8	More Details
CVE-2019-13204	Some Kyocera printers (such as the ECOSYS M5526cdw 2R7_2000.001.701) were affected by multiple buffer overflow vulnerabilities in the IPP service. This would allow an unauthenticated attacker to cause a Denial of Service (DoS), and potentially execute arbitrary code on the device.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0872	A remote code execution vulnerability exists in Application Inspector version v1.0.23 or earlier when the tool reflects example code snippets from third-party source files into its HTML output, aka 'Remote Code Execution Vulnerability in Application Inspector'.	9.6	More Details
CVE-2020-10594	An issue was discovered in drf-jwt 1.15.x before 1.15.1. It allows attackers with access to a notionally invalidated token to obtain a new, working token via the refresh endpoint, because the blacklist protection mechanism is incompatible with the token-refresh feature. NOTE: drf-jwt is a fork of jpadilla/django-rest-framework-jwt, which is unmaintained.	9.1	More Details
CVE-2020-1887	Incorrect validation of the TLS SNI hostname in osquery versions after 2.9.0 and before 4.2.0 could allow an attacker to MITM osquery traffic in the absence of a configured root chain of trust.	9.1	More Details
CVE-2019-5160	An exploitable improper host validation vulnerability exists in the Cloud Connectivity functionality of WAGO PFC200 Firmware versions 03.02.02(14), 03.01.07(13), and 03.00.39(12). A specially crafted HTTPS POST request can cause the software to connect to an unauthorized host, resulting in unauthorized access to firmware update functionality. An attacker can send an authenticated HTTPS POST request to direct the Cloud Connectivity software to connect to an attacker controlled Azure IoT Hub node.	9.1	More Details
CVE-2019-14887	A flaw was found when an OpenSSL security provider is used with Wildfly, the 'enabled-protocols' value in the Wildfly configuration isn't honored. An attacker could target the traffic sent from Wildfly and downgrade the connection to a weaker version of TLS, potentially breaking the encryption. This could lead to a leak of the data being passed over the network. Wildfly version 7.2.0.GA, 7.2.3.GA and 7.2.5.CR2 are believed to be vulnerable.	9.1	More Details
CVE-2020-10083	GitLab 12.7 through 12.8.1 has Insecure Permissions. Under certain conditions involving groups, project authorization changes were not being applied.	9.1	More Details
CVE-2020-10117	cPanel before 84.0.20 mishandles enforcement of demo checks in the Market UAPI namespace (SEC-542).	9.1	More Details
CVE-2020-10118	cPanel before 84.0.20 allows a demo account to modify files via Branding API calls (SEC-543).	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-5161	An exploitable remote code execution vulnerability exists in the Cloud Connectivity functionality of WAGO PFC200 versions 03.02.02(14), 03.01.07(13), and 03.00.39(12). A specially crafted XML file will direct the Cloud Connectivity service to download and execute a shell script with root privileges.	9.1	More Details
CVE-2019-18578	Dell EMC XtremIO XMS versions prior to 6.3.0 contain a stored cross-site scripting vulnerability. A low-privileged malicious remote user of XtremIO may exploit this vulnerability to store malicious HTML or JavaScript code in application fields. When victim users access the injected page through their browsers, the malicious code may be executed by the web browser in the context of the vulnerable web application.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-9471	Umbraco Cloud 8.5.3 allows an authenticated file upload (and consequently Remote Code Execution) via the Install Packages functionality.	8.8	More Details
CVE-2019-10808	utilitify prior to 1.0.3 allows modification of object properties. The merge method could be tricked into adding or modifying properties of the Object.prototype.	8.8	More Details
CVE-2020-9436	PHOENIX CONTACT TC ROUTER 3002T-4G through 2.05.3, TC ROUTER 2002T-3G through 2.05.3, TC ROUTER 3002T-4G VZW through 2.05.3, TC ROUTER 3002T-4G ATT through 2.05.3, TC CLOUD CLIENT 1002-4G through 2.03.17, and TC CLOUD CLIENT 1002-TXTX through 1.03.17 devices allow authenticated users to inject system commands through a modified POST request to a specific URL.	8.8	More Details
CVE-2020-5546	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability in TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier allows an attacker on the same network segment to stop the network functions or execute malware via a specially crafted packet.	8.8	More Details
CVE-2019-17654	An Insufficient Verification of Data Authenticity vulnerability in FortiManager 6.2.1, 6.2.0, 6.0.6 and below may allow an unauthenticated attacker to perform a Cross-Site WebSocket Hijacking (CSWSH) attack.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9346	Zoho ManageEngine Password Manager Pro 10.4 and prior has no protection against Cross-site Request Forgery (CSRF) attacks, as demonstrated by changing a user's role.	8.8	More Details
CVE-2020-0807	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0801, CVE-2020-0809, CVE-2020-0869.	8.8	More Details
CVE-2020-0809	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0801, CVE-2020-0807, CVE-2020-0869.	8.8	More Details
CVE-2019-20452	A problem was found in Pydio Core before 8.2.4 and Pydio Enterprise before 8.2.4. A PHP object injection is present in the page plugins/core.access/src/RecycleBinManager.php. An authenticated user with basic privileges can inject objects and achieve remote code execution.	8.8	More Details
CVE-2019-20453	A problem was found in Pydio Core before 8.2.4 and Pydio Enterprise before 8.2.4. A PHP object injection is present in the page plugins/uploader.http/HttpDownload.php. An authenticated user with basic privileges can inject objects and achieve remote code execution.	8.8	More Details
CVE-2018-21037	Subrion CMS 4.1.5 (and possibly earlier versions) allow CSRF to change the administrator password via the panel/members/edit/1 URI.	8.8	More Details
CVE-2019-20492	cPanel before 82.0.18 allows authentication bypass because of misparsing of the format of the password file (SEC-516).	8.8	More Details
CVE-2020-0816	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'.	8.8	More Details
CVE-2020-8141	The dot package v1.1.2 uses Function() to compile templates. This can be exploited by the attacker if they can control the given template or if they can control the value set on Object.prototype.	8.8	More Details
CVE-2020-10478	CSRF in admin/manage-settings.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to change the global settings, potentially gaining code execution or causing a denial of service, via a crafted request.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10568	The sitepress-multilingual-cms (WPML) plugin before 4.3.7-b.2 for WordPress has CSRF due to a loose comparison. This leads to remote code execution in includes/class-wp-installer.php via a series of requests that leverage unintended comparisons of integers to strings.	8.8	More Details
CVE-2019-13196	Some Kyocera printers (such as the ECOSYS M5526cdw 2R7_2000.001.701) were affected by a buffer overflow vulnerability in the arg4 and arg9 parameters of several functionalities of the web application that would allow an authenticated attacker to perform a Denial of Service attack, crashing the device, or potentially execute arbitrary code on the device.	8.8	More Details
CVE-2020-0850	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0851, CVE-2020-0852, CVE-2020-0855, CVE-2020-0892.	8.8	More Details
CVE-2019-13193	Some Brother printers (such as the HL-L8360CDW v1.20) were affected by a stack buffer overflow vulnerability as the web server did not parse the cookie value properly. This would allow an attacker to execute arbitrary code on the device.	8.8	More Details
CVE-2019-13395	The Voo branded NETGEAR CG3700b custom firmware V2.02.03 allows CSRF against all /goform/ URIs. An attacker can modify all settings including WEP/WPA/WPA2 keys, restore the router to factory settings, or even upload an entire malicious configuration file.	8.8	More Details
CVE-2019-13206	Some Kyocera printers (such as the ECOSYS M5526cdw 2R7_2000.001.701) were affected by a buffer overflow vulnerability in multiple parameters of the Document Boxes functionality of the web application that would allow an authenticated attacker to perform a Denial of Service attack, crashing the device, or potentially execute arbitrary code on the device.	8.8	More Details
CVE-2019-13203	Some Kyocera printers (such as the ECOSYS M5526cdw 2R7_2000.001.701) were affected by an integer overflow vulnerability in the arg3 parameter of several functionalities of the web application that would allow an authenticated attacker to perform a Denial of Service attack, crashing the device, or potentially execute arbitrary code on the device.	8.8	More Details
CVE-2020-10540	Untis WebUntis before 2020.9.6 allows CSRF for certain combinations of rights and modules.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-17653	A Cross-Site Request Forgery (CSRF) vulnerability in the user interface of Fortinet FortiSIEM 5.2.5 could allow a remote, unauthenticated attacker to perform arbitrary actions using an authenticated user's session by persuading the victim to follow a malicious link.	8.8	More Details
CVE-2020-0583	Improper access control in the subsystem for Intel(R) Smart Sound Technology may allow an authenticated user to potentially enable escalation of privilege via local access. This affects Intel® Smart Sound Technology before versions: 10th Generation Intel® Core™ i7 Processors, version 3431 and 8th Generation Intel® Core™ Processors, version 3349.	8.8	More Details
CVE-2020-0869	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0801, CVE-2020-0807, CVE-2020-0809.	8.8	More Details
CVE-2020-0881	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0883.	8.8	More Details
CVE-2020-0883	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0881.	8.8	More Details
CVE-2020-10531	An issue was discovered in International Components for Unicode (ICU) for C/C++ through 66.1. An integer overflow, leading to a heap-based buffer overflow, exists in the UnicodeString::doAppend() function in common/unistr.cpp.	8.8	More Details
CVE-2020-0801	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0807, CVE-2020-0809, CVE-2020-0869.	8.8	More Details
CVE-2019-20490	cPanel before 82.0.18 allows authentication bypass because webmail usernames are processed inconsistently (SEC-499).	8.8	More Details
CVE-2019-9102	An issue was discovered on Moxa MGate MB3170 and MB3270 devices before 4.1, MB3280 and MB3480 devices before 3.1, MB3660 devices before 2.3, and MB3180 devices before 2.1. A predictable mechanism of generating tokens allows remote attackers to bypass the cross-site request forgery (CSRF) protection mechanism.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10557	An issue was discovered in AContent through 1.4. It allows the user to run commands on the server with a low-privileged account. The upload section in the file manager page contains an arbitrary file upload vulnerability via upload.php. The extension .php7 bypasses file upload restrictions.	8.8	More Details
CVE-2020-0684	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.	8.8	More Details
CVE-2020-3947	VMware Workstation (15.x before 15.5.2) and Fusion (11.x before 11.5.2) contain a use-after vulnerability in vmnetdhcp. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition of the vmnetdhcp service running on the host machine.	8.8	More Details
CVE-2020-9408	The Spotfire library component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains a vulnerability that theoretically allows an attacker with write permissions to the Spotfire Library, but not "Script Author" group permission, to modify attributes of files and objects saved to the library such that the system treats them as trusted. This could allow an attacker to cause the Spotfire Web Player, Analyst clients, and TERR Service into executing arbitrary code with the privileges of the system account that started those processes. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 10.8.0 and below and TIBCO Spotfire Server: versions 7.11.9 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.3.0, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, and 10.3.6, versions 10.4.0, 10.5.0, 10.6.0, 10.6.1, 10.7.0, and 10.8.0.	8.8	More Details
CVE-2020-6585	Nagios Log Server 2.1.3 has CSRF.	8.8	More Details
CVE-2020-10241	An issue was discovered in Joomla! before 3.9.16. Missing token checks in the image actions of com_templates lead to CSRF.	8.8	More Details
CVE-2020-10239	An issue was discovered in Joomla! before 3.9.16. Incorrect Access Control in the SQL fieldtype of com_fields allows access for non-superadmin users.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9543	OpenStack Manila <7.4.1, >=8.0.0 <8.1.1, and >=9.0.0 <9.1.1 allows attackers to view, update, delete, or share resources that do not belong to them, because of a context-free lookup of a UUID. Attackers may also create resources, such as shared file systems and groups of shares on such share networks.	8.3	More Details
CVE-2020-1979	A format string vulnerability in the PAN-OS log daemon (logd) on Panorama allows a network based attacker with knowledge of registered firewall devices and access to Panorama management interfaces to execute arbitrary code, bypassing the restricted shell and escalating privileges. This issue affects only PAN-OS 8.1 versions earlier than PAN-OS 8.1.13 on Panorama. This issue does not affect PAN-OS 7.1, PAN-OS 9.0, or later PAN-OS versions.	8.1	More Details
CVE-2020-10088	GitLab 12.5 through 12.8.1 has Insecure Permissions. Depending on particular group settings, it was possible for invited groups to be given the incorrect permission level.	8.1	More Details
CVE-2020-8435	An issue was discovered in the RegistrationMagic plugin 4.6.0.0 for WordPress. There is SQL injection via the rm_analytics_show_form rm_form_id parameter.	8.1	More Details
CVE-2020-7982	An issue was discovered in OpenWrt 18.06.0 to 18.06.6 and 19.07.0, and LEDE 17.01.0 to 17.01.7. A bug in the fork of the opkg package manager before 2020-01-25 prevents correct parsing of embedded checksums in the signed repository index, allowing a man-in-the-middle attacker to inject arbitrary package payloads (which are installed without verification).	8.1	More Details
CVE-2019-19821	A post-authentication privilege escalation in the web application of Combodo iTop allows regular authenticated users to access information and modify information with administrative privileges by not following the HTTP Location header in server responses. This is fixed in all iTop packages (community, essential, professional) in versions : 2.5.4, 2.6.3, 2.7.0	8.1	More Details
CVE-2020-0905	An remote code execution vulnerability exists in Microsoft Dynamics Business Central, aka 'Dynamics Business Central Remote Code Execution Vulnerability'.	8.0	More Details
CVE-2019-19756	An internal product security audit of Lenovo XClarity Administrator (LXCA) discovered Windows OS credentials, used to perform driver updates of managed systems, being written to a log file in clear text. This only affects LXCA version 2.6.0 when performing a Windows driver update. Affected logs are only accessible to authorized users in the First Failure Data Capture (FFDC) service log and log files on LXCA.	7.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0868	An elevation of privilege vulnerability exists when the Windows Update Orchestrator Service improperly handles file operations, aka 'Windows Update Orchestrator Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0867.	7.8	More Details
CVE-2020-0780	An elevation of privilege vulnerability exists in the way that the Windows Network List Service handles objects in memory, aka 'Windows Network List Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0897	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0777, CVE-2020-0797, CVE-2020-0800, CVE-2020-0864, CVE-2020-0865, CVE-2020-0866.	7.8	More Details
CVE-2020-0791	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0898.	7.8	More Details
CVE-2020-0896	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0840, CVE-2020-0841, CVE-2020-0849.	7.8	More Details
CVE-2020-0857	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0788	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0877, CVE-2020-0887.	7.8	More Details
CVE-2020-0858	An elevation of privilege vulnerability exists when the &quot;Public Account Pictures&quot; folder improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0776.	7.8	More Details
CVE-2020-0892	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0850, CVE-2020-0851, CVE-2020-0852, CVE-2020-0855.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3950	VMware Fusion (11.x before 11.5.2), VMware Remote Console for Mac (11.x and prior before 11.0.1) and Horizon Client for Mac (5.x and prior before 5.4.0) contain a privilege escalation vulnerability due to improper use of setuid binaries. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMRC or Horizon Client is installed.	7.8	More Details
CVE-2020-0860	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows ActiveX Installer Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0770, CVE-2020-0773.	7.8	More Details
CVE-2020-0861	An information disclosure vulnerability exists when the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability'.	7.8	More Details
CVE-2020-0777	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0797, CVE-2020-0800, CVE-2020-0864, CVE-2020-0865, CVE-2020-0866, CVE-2020-0897.	7.8	More Details
CVE-2020-0887	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0788, CVE-2020-0877.	7.8	More Details
CVE-2020-0864	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0777, CVE-2020-0797, CVE-2020-0800, CVE-2020-0865, CVE-2020-0866, CVE-2020-0897.	7.8	More Details
CVE-2020-0776	An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0858.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20326	A heap-based buffer overflow in _cairo_image_surface_create_from_jpeg() in extensions/cairo_io/cairo-image-surface-jpeg.c in GNOME gThumb before 3.8.3 and Linux Mint Pix before 2.4.5 allows attackers to cause a crash and potentially execute arbitrary code via a crafted JPEG file.	7.8	More Details
CVE-2020-0787	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) improperly handles symbolic links, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0778	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0802, CVE-2020-0803, CVE-2020-0804, CVE-2020-0845.	7.8	More Details
CVE-2020-0877	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0788, CVE-2020-0887.	7.8	More Details
CVE-2020-0865	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0777, CVE-2020-0797, CVE-2020-0800, CVE-2020-0864, CVE-2020-0866, CVE-2020-0897.	7.8	More Details
CVE-2020-0866	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0777, CVE-2020-0797, CVE-2020-0800, CVE-2020-0864, CVE-2020-0865, CVE-2020-0897.	7.8	More Details
CVE-2020-0867	An elevation of privilege vulnerability exists when the Windows Update Orchestrator Service improperly handles file operations, aka 'Windows Update Orchestrator Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0868.	7.8	More Details
CVE-2020-0855	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0850, CVE-2020-0851, CVE-2020-0852, CVE-2020-0892.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0800	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0777, CVE-2020-0797, CVE-2020-0864, CVE-2020-0865, CVE-2020-0866, CVE-2020-0897.	7.8	More Details
CVE-2020-0852	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0850, CVE-2020-0851, CVE-2020-0855, CVE-2020-0892.	7.8	More Details
CVE-2020-0770	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows ActiveX Installer Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0773, CVE-2020-0860.	7.8	More Details
CVE-2020-0799	An elevation of privilege vulnerability exists in Microsoft Windows when the Windows kernel fails to properly handle parsing of certain symbolic links, aka 'Windows Kernel Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0802	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0778, CVE-2020-0803, CVE-2020-0804, CVE-2020-0845.	7.8	More Details
CVE-2020-0803	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0778, CVE-2020-0802, CVE-2020-0804, CVE-2020-0845.	7.8	More Details
CVE-2020-0798	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0779, CVE-2020-0814, CVE-2020-0842, CVE-2020-0843.	7.8	More Details
CVE-2020-0762	An elevation of privilege vulnerability exists when Windows Defender Security Center handles certain objects in memory.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Windows Defender Security Center Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0763.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0804	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0778, CVE-2020-0802, CVE-2020-0803, CVE-2020-0845.	7.8	More Details
CVE-2020-0806	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0772.	7.8	More Details
CVE-2020-0763	An elevation of privilege vulnerability exists when Windows Defender Security Center handles certain objects in memory.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Windows Defender Security Center Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0762.	7.8	More Details
CVE-2020-0797	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0777, CVE-2020-0800, CVE-2020-0864, CVE-2020-0865, CVE-2020-0866, CVE-2020-0897.	7.8	More Details
CVE-2020-0808	An elevation of privilege vulnerability exists in the way the Provisioning Runtime validates certain file operations, aka 'Provisioning Runtime Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0793	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0810	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector allows file creation in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system.An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.The update addresses the vulnerability by not permitting Diagnostics Hub Standard Collector or the Visual Studio Standard Collector to create files in arbitrary locations., aka 'Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0769	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0771.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0814	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0779, CVE-2020-0798, CVE-2020-0842, CVE-2020-0843.	7.8	More Details
CVE-2020-0851	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0850, CVE-2020-0852, CVE-2020-0855, CVE-2020-0892.	7.8	More Details
CVE-2020-0898	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0791.	7.8	More Details
CVE-2020-0819	An elevation of privilege vulnerability exists when the Windows Device Setup Manager improperly handles file operations, aka 'Windows Device Setup Manager Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0822	An elevation of privilege vulnerability exists when the Windows Language Pack Installer improperly handles file operations, aka 'Windows Language Pack Installer Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0771	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0769.	7.8	More Details
CVE-2020-0834	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0840	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0841, CVE-2020-0849, CVE-2020-0896.	7.8	More Details
CVE-2020-0841	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0840, CVE-2020-0849, CVE-2020-0896.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0842	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0779, CVE-2020-0798, CVE-2020-0814, CVE-2020-0843.	7.8	More Details
CVE-2020-0843	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0779, CVE-2020-0798, CVE-2020-0814, CVE-2020-0842.	7.8	More Details
CVE-2020-0844	An elevation of privilege vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability'.	7.8	More Details
CVE-2020-0845	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0778, CVE-2020-0802, CVE-2020-0803, CVE-2020-0804.	7.8	More Details
CVE-2020-0772	An elevation of privilege vulnerability exists when Windows Error Reporting improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0806.	7.8	More Details
CVE-2020-0773	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows ActiveX Installer Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0770, CVE-2020-0860.	7.8	More Details
CVE-2020-0849	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0840, CVE-2020-0841, CVE-2020-0896.	7.8	More Details
CVE-2020-0781	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly handles objects in memory, aka 'Windows UPnP Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0783.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0504	Buffer overflow in Intel(R) Graphics Drivers before versions 15.40.44.5107, 15.45.30.5103, and 26.20.100.7158 may allow an authenticated user to potentially enable escalation of privilege and denial of service via local access.	7.8	More Details
CVE-2020-9290	An Unsafe Search Path vulnerability in FortiClient for Windows online installer 6.2.3 and below may allow a local attacker with control over the directory in which FortiClientOnlineInstaller.exe and FortiClientVPNOnlineInstaller.exe resides to execute arbitrary code on the system via uploading malicious Filter Library DLL files in that directory.	7.8	More Details
CVE-2019-5181	An exploitable stack buffer overflow vulnerability vulnerability exists in the iocheckd service ‘I/O-Check’ functionality of WAGO PFC 200 Firmware version 03.02.02(14). A specially crafted XML cache file written to a specific location on the device can cause a stack buffer overflow, resulting in code execution. An attacker can send a specially crafted packet to trigger the parsing of this cache file. The destination buffer sp+0x440 is overflowed with the call to sprintf() for any subnetmask values that are greater than 1024-len(‘/etc/config-tools/config_interfaces interface=X1 state=enabled subnet-mask=‘) in length. A subnetmask value of length 0x3d9 will cause the service to crash.	7.8	More Details
CVE-2019-5167	An exploitable command injection vulnerability exists in the iocheckd service ‘I/O-Check’ function of the WAGO PFC 200 version 03.02.02(14). At 0x1e3f0 the extracted dns value from the xml file is used as an argument to /etc/config-tools/edit_dns_server %s dns-server-nr=%d dns-server-name=<contents of dns node> using sprintf(). This command is later executed via a call to system(). This is done in a loop and there is no limit to how many dns entries will be parsed from the xml file.	7.8	More Details
CVE-2019-5168	An exploitable command injection vulnerability exists in the iocheckd service ‘I/O-Check’ function of the WAGO PFC 200 version 03.02.02(14). An attacker can send a specially crafted XML cache file At 0x1e8a8 the extracted domainname value from the xml file is used as an argument to /etc/config-tools/edit_dns_server domain-name=<contents of domainname node> using sprintf().This command is later executed via a call to system().	7.8	More Details
CVE-2020-10565	grub2-bhyve, as used in FreeBSD bhyve before revision 525916 2020-02-12, does not validate the address provided as part of a memrw command (read_* or write_*) by a guest through a grub2.cfg file. This allows an untrusted guest to perform arbitrary read or write operations in the context of the grub-bhyve process, resulting in code execution as root on the host OS.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10566	grub2-bhyve, as used in FreeBSD bhyve before revision 525916 2020-02-12, mishandles font loading by a guest through a grub2.cfg file, leading to a buffer overflow.	7.8	More Details
CVE-2020-5958	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which an attacker with local system access can plant a malicious DLL file, which may lead to code execution, denial of service, or information disclosure.	7.8	More Details
CVE-2019-5172	An exploitable command injection vulnerability exists in the iocheckd service 'I/O-Check' function of the WAGO PFC 200 Firmware version 03.02.02(14). An attacker can send a specially crafted packet to trigger the parsing of this cache file. At 0x1e840 the extracted ntp value from the xml file is used as an argument to /etc/config-tools/config_sntp time-server-%d=<contents of ntp node> using sprintf(). This command is later executed via a call to system(). This is done in a loop and there is no limit to how many ntp entries will be parsed from the xml file.	7.8	More Details
CVE-2019-5173	An exploitable command injection vulnerability exists in the iocheckd service 'I/O-Check' function of the WAGO PFC 200 Firmware version 03.02.02(14). A specially crafted XML cache file written to a specific location on the device can be used to inject OS commands. An attacker can send a specially crafted packet to trigger the parsing of this cache file. At 0x1e9fc the extracted state value from the xml file is used as an argument to /etc/config-tools/config_interfaces interface=X1 state=<contents of state node> using sprintf(). This command is later executed via a call to system().	7.8	More Details
CVE-2019-5174	An exploitable command injection vulnerability exists in the iocheckd service 'I/O-Check' function of the WAGO PFC 200 version 03.02.02(14). A specially crafted XML cache file written to a specific location on the device can be used to inject OS commands. An attacker can send a specially crafted packet to trigger the parsing of this cache file.At 0x1e9fc the extracted subnetmask value from the xml file is used as an argument to /etc/config-tools/config_interfaces interface=X1 state=enabled subnet-mask=<contents of subnetmask node> using sprintf(). This command is later executed via a call to system().	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-5175	An exploitable command injection vulnerability exists in the iocheckd service ‘I/O-Check’ function of the WAGO PFC 200 Firmware version 03.02.02(14). A specially crafted XML cache file written to a specific location on the device can be used to inject OS commands. An attacker can send a specially crafted packet to trigger the parsing of this cache file.At 0x1ea28 the extracted type value from the xml file is used as an argument to /etc/config-tools/config_interfaces interface=X1 state=enabled config-type=<contents of type node> using sprintf(). This command is later executed via a call to system().	7.8	More Details
CVE-2019-5169	An exploitable command injection vulnerability exists in the iocheckd service ‘I/O-Check’ function of the WAGO PFC 200 Firmware version 03.02.02(14). A specially crafted XML cache file written to a specific location on the device can be used to inject OS commands. An attacker can send a specially crafted packet to trigger the parsing of this cache file. At 0x1e900 the extracted gateway value from the xml file is used as an argument to /etc/config-tools/config_default_gateway number=0 state=enabled value=<contents of gateway node> using sprintf(). This command is later executed via a call to system().	7.8	More Details
CVE-2019-5158	An exploitable firmware downgrade vulnerability exists in the firmware update package functionality of the WAGO e!COCKPIT automation software v1.6.1.5. A specially crafted firmware update file can allow an attacker to install an older firmware version while the user thinks a newer firmware version is being installed. An attacker can create a custom firmware update package with invalid metadata in order to trigger this vulnerability.	7.8	More Details
CVE-2019-5170	An exploitable command injection vulnerability exists in the iocheckd service ‘I/O-Check’ function of the WAGO PFC 200 Firmware version 03.02.02(14). A specially crafted XML cache file written to a specific location on the device can be used to inject OS commands. An attacker can send a specially crafted packet to trigger the parsing of this cache file.At 0x1e87c the extracted hostname value from the xml file is used as an argument to /etc/config-tools/change_hostname hostname=<contents of hostname node> using sprintf(). This command is later executed via a call to system().	7.8	More Details
CVE-2019-5171	An exploitable command injection vulnerability exists in the iocheckd service ‘I/O-Check’ function of the WAGO PFC 200 Firmware version 03.02.02(14). An attacker can send specially crafted packet at 0x1ea48 to the extracted hostname value from the xml file that is used as an argument to /etc/config-tools/config_interfaces interface=X1 state=enabled ip-address=<contents of ip node> using sprintf().	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9287	An Unsafe Search Path vulnerability in FortiClient EMS online installer 6.2.1 and below may allow a local attacker with control over the directory in which FortiClientEMSOnlineInstaller.exe resides to execute arbitrary code on the system via uploading malicious Filter Library DLL files in that directory.	7.8	More Details
CVE-2019-5178	An exploitable stack buffer overflow vulnerability vulnerability exists in the iocheckd service ‘I/O-Check’ functionality of WAGO PFC 200 Firmware version 03.02.02(14). An attacker can send a specially crafted packet to trigger the parsing of this cache file. The destination buffer sp+0x440 is overflowed with the call to sprintf() for any hostname values that are greater than 1024-len(‘/etc/config-tools/change_hostname hostname=‘) in length. A hostname value of length 0x3fd will cause the service to crash.	7.8	More Details
CVE-2020-10587	antiX and MX Linux allow local users to achieve root access via "persist-config --command /bin/sh" because of the Sudo configuration.	7.8	More Details
CVE-2020-10588	v2rayL 2.1.3 allows local users to achieve root access because /etc/v2rayL/add.sh and /etc/v2rayL/remove.sh are owned by a low-privileged user but execute as root via Sudo.	7.8	More Details
CVE-2019-5179	An exploitable stack buffer overflow vulnerability vulnerability exists in the iocheckd service ‘I/O-Check’ functionality of WAGO PFC 200 Firmware version 03.02.02(14). An attacker can send a specially crafted packet to trigger the parsing of this cache file.	7.8	More Details
CVE-2020-10589	v2rayL 2.1.3 allows local users to achieve root access because /etc/v2rayL/config.json is owned by a low-privileged user but contains commands that are executed as root, after v2rayL.service is restarted via Sudo.	7.8	More Details
CVE-2019-5180	An exploitable stack buffer overflow vulnerability vulnerability exists in the iocheckd service ‘I/O-Check’ functionality of WAGO PFC 200 Firmware version 03.02.02(14). An attacker can send a specially crafted packet to trigger the parsing of this cache file. The destination buffer sp+0x440 is overflowed with the call to sprintf() for any ip values that are greater than 1024-len(‘/etc/config-tools/config_interfaces interface=X1 state=enabled ip-address=‘) in length. A ip value of length 0x3da will cause the service to crash.	7.8	More Details
CVE-2019-2089	In app uninstallation, there is a possible set of permissions that may not be removed from a shared app ID. This could lead to a local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android Versions: Android-10 Android ID: A-116608833	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-5159	An exploitable improper input validation vulnerability exists in the firmware update functionality of WAGO e!COCKPIT automation software v1.6.0.7. A specially crafted firmware update file can allow an attacker to write arbitrary files to arbitrary locations on WAGO controllers as a part of executing a firmware update, potentially resulting in code execution. An attacker can create a malicious firmware update package file using any zip utility. The user must initiate a firmware update through e!COCKPIT and choose the malicious wup file using the file browser to trigger the vulnerability.	7.8	More Details
CVE-2019-5166	An exploitable stack buffer overflow vulnerability exists in the iocheckd service 'I/O-Check' functionality of WAGO PFC 200 version 03.02.02(14). A specially crafted XML cache file written to a specific location on the device can cause a stack buffer overflow, resulting in code execution. An attacker can send a specially crafted packet to trigger the parsing of this cache file.	7.8	More Details
CVE-2020-0530	Improper buffer restrictions in firmware for Intel(R) NUC may allow an authenticated user to potentially enable escalation of privilege via local access. The list of affected products is provided in intel-sa-00343: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00343.html	7.8	More Details
CVE-2019-5543	For VMware Horizon Client for Windows (5.x and prior before 5.3.0), VMware Remote Console for Windows (10.x before 11.0.0), VMware Workstation for Windows (15.x before 15.5.2) the folder containing configuration files for the VMware USB arbitration service was found to be writable by all users. A local user on the system where the software is installed may exploit this issue to run commands as any user.	7.8	More Details
CVE-2020-0520	Path traversal in igdkmd64.sys for Intel(R) Graphics Drivers before versions 15.45.30.5103, 15.40.44.5107, 15.36.38.5117 and 15.33.49.5100 may allow an authenticated user to potentially enable escalation of privilege or denial of service via local access.	7.8	More Details
CVE-2020-0514	Improper default permissions in the installer for Intel(R) Graphics Drivers before versions 26.20.100.7463 and 15.45.30.5103 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-0508	Incorrect default permissions in the installer for Intel(R) Graphics Drivers before versions 15.33.49.5100, 15.36.38.5117, 15.40.44.5107, 15.45.30.5103, and 26.20.100.7212 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0546	Unquoted service path in Intel(R) Optane(TM) DC Persistent Memory Module Management Software before version 1.0.0.3461 may allow an authenticated user to potentially enable escalation of privilege and denial of service via local access.	7.8	More Details
CVE-2020-0565	Uncontrolled search path in Intel(R) Graphics Drivers before version 26.20.100.7158 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-3948	Linux Guest VMs running on VMware Workstation (15.x before 15.5.2) and Fusion (11.x before 11.5.2) contain a local privilege escalation vulnerability due to improper file permissions in Cortado Thinprint. Local attackers with non-administrative access to a Linux guest VM with virtual printing enabled may exploit this issue to elevate their privileges to root on the same guest VM.	7.8	More Details
CVE-2020-8469	Trend Micro Password Manager for Windows version 5.0 is affected by a DLL hijacking vulnerability would could potentially allow an attacker privleged escalation.	7.8	More Details
CVE-2020-0515	Uncontrolled search path element in the installer for Intel(R) Graphics Drivers before versions 26.20.100.7584, 15.45.30.5103, 15.40.44.5107, 15.36.38.5117, and 15.33.49.5100 may allow an authenticated user to potentially enable escalation of privilege via local access	7.8	More Details
CVE-2020-0519	Improper access control for Intel(R) Graphics Drivers before versions 15.33.49.5100 and 15.36.38.5117 may allow an authenticated user to potentially enable escalation of privilege or denial of service via local access.	7.8	More Details
CVE-2020-1980	A shell command injection vulnerability in the PAN-OS CLI allows a local authenticated user to escape the restricted shell and escalate privileges. This issue affects only PAN-OS 8.1 versions earlier than PAN-OS 8.1.13. This issue does not affect PAN-OS 7.1, PAN-OS 9.0, or later PAN-OS versions. This issue is fixed in PAN-OS 8.1.13, and all later versions.	7.8	More Details
CVE-2020-0783	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly handles objects in memory, aka 'Windows UPnP Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0781.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5257	In Administrate (rubygem) before version 0.13.0, when sorting by attributes on a dashboard, the direction parameter was not validated before being interpolated into the SQL query. This could present a SQL injection if the attacker were able to modify the `direction` parameter and bypass ActiveRecord SQL protections. Whilst this does have a high-impact, to exploit this you need access to the Administrate dashboards, which we would expect to be behind authentication. This is patched in wersion 0.13.0.	7.7	More Details
CVE-2020-7254	Privilege Escalation vulnerability in the command line interface in McAfee Advanced Threat Defense (ATD) 4.x prior to 4.8.2 allows local users to execute arbitrary code via improper access controls on the sudo command.	7.7	More Details
CVE-2020-5240	In wagtail-2fa before 1.4.1, any user with access to the CMS can view and delete other users 2FA devices by going to the correct path. The user does not require special permissions in order to do so. By deleting the other users device they can disable the target users 2FA devices and potentially compromise the account if they figure out their password. The problem has been patched in version 1.4.1.	7.6	More Details
CVE-2017-12842	Bitcoin Core before 0.14 allows an attacker to create an ostensibly valid SPV proof for a payment to a victim who uses an SPV wallet, even if that payment did not actually occur. Completing the attack would cost more than a million dollars, and is relevant mainly only in situations where an autonomous system relies solely on an SPV proof for transactions of a greater dollar amount.	7.5	More Details
CVE-2020-0811	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based)L, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0812.	7.5	More Details
CVE-2020-9321	configurationwatcher.go in Traefik 2.x before 2.1.4 and TraefikEE 2.0.0 mishandles the purging of certificate contents from providers before logging.	7.5	More Details
CVE-2018-13063	Easy!Appointments 1.3.0 has a Missing Authorization issue allowing retrieval of hashed passwords and salts.	7.5	More Details
CVE-2019-9474	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-10 Android ID: A-79996267	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6582	Nagios NRPE 3.2.1 has a Heap-Based Buffer Overflow, as demonstrated by interpretation of a small negative number as a large positive number during a bzero call.	7.5	More Details
CVE-2020-5849	Unraid 6.8.0 allows authentication bypass.	7.5	More Details
CVE-2019-19209	Dolibarr ERP/CRM before 10.0.3 allows SQL Injection.	7.5	More Details
CVE-2019-19945	uhttpd in OpenWrt through 18.06.5 and 19.x through 19.07.0-rc2 has an integer signedness error. This leads to out-of-bounds access to a heap buffer and a subsequent crash. It can be triggered with an HTTP POST request to a CGI script, specifying both "Transfer-Encoding: chunked" and a large negative Content-Length value.	7.5	More Details
CVE-2020-6988	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, A remote, unauthenticated attacker can send a request from the RSLogix 500 software to the victim's MicroLogix controller. The controller will then respond to the client with used password values to authenticate the user on the client-side. This method of authentication may allow an attacker to bypass authentication altogether, disclose sensitive information, or leak credentials.	7.5	More Details
CVE-2020-6984	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic function utilized to protect the password in MicroLogix is discoverable.	7.5	More Details
CVE-2020-10238	An issue was discovered in Joomla! before 3.9.16. Various actions in com_templates lack the required ACL checks, leading to various potential attack vectors.	7.5	More Details
CVE-2019-19942	Missing output sanitation in Swisscom Centro Grande Centro Grande before 6.16.12, Centro Business 1.0 (ADB) before 7.10.18, and Centro Business 2.0 before 8.02.04 allows a remote attacker to perform DNS spoofing against the web interface via crafted hostnames in DHCP requests.	7.5	More Details
CVE-2020-0812	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based)L, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0811.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10578	An arbitrary file read vulnerability exists in system/controller/backend/template.php in QCMS v3.0.1.	7.5	More Details
CVE-2019-9473	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-10 Android ID: A-115363533	7.5	More Details
CVE-2020-0813	An information disclosure vulnerability exists when Chakra improperly discloses the contents of its memory, which could provide an attacker with information to further compromise the userâ€™s computer or data.To exploit the vulnerability, an attacker must know the memory address of where the object was created.The update addresses the vulnerability by changing the way certain functions handle objects in memory., aka 'Scripting Engine Information Disclosure Vulnerability'.	7.5	More Details
CVE-2020-0848	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0768, CVE-2020-0823, CVE-2020-0825, CVE-2020-0826, CVE-2020-0827, CVE-2020-0828, CVE-2020-0829, CVE-2020-0830, CVE-2020-0831, CVE-2020-0832, CVE-2020-0833.	7.5	More Details
CVE-2019-13195	The web application of some Kyocera printers (such as the ECOSYS M5526cdw 2R7_2000.001.701) was vulnerable to path traversal, allowing an unauthenticated user to retrieve arbitrary files, or check if files or folders existed within the file system.	7.5	More Details
CVE-2019-13194	Some Brother printers (such as the HL-L8360CDW v1.20) were affected by different information disclosure vulnerabilities that provided sensitive information to an unauthenticated user who visits a specific URL.	7.5	More Details
CVE-2019-13166	Some Xerox printers (such as the Phaser 3320 V53.006.16.000) did not implement account lockout. Local account credentials may be extracted from the device via brute force guessing attacks.	7.5	More Details
CVE-2020-10073	GitLab EE 12.4.2 through 12.8.1 allows Denial of Service. It was internally discovered that a potential denial of service involving permissions checks could impact a project home page.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-13393	The Voo branded NETGEAR CG3700b custom firmware V2.02.03 uses the same default 8 character passphrase for the administrative console and the WPA2 pre-shared key. Either an attack against HTTP Basic Authentication or an attack against WPA2 could be used to determine this passphrase.	7.5	More Details
CVE-2019-13205	All configuration parameters of certain Kyocera printers (such as the ECOSYS M5526cdw 2R7_2000.001.701) were accessible by unauthenticated users. This information was only presented in the menus when authenticated, and the pages that loaded this information were also protected. However, all files that contained the configuration parameters were accessible. These files contained sensitive information, such as users, community strings, and other passwords configured in the printer.	7.5	More Details
CVE-2020-10089	GitLab 8.11 through 12.8.1 allows a Denial of Service when using several features to recursively request eachother,	7.5	More Details
CVE-2020-10087	GitLab before 12.8.2 allows Information Disclosure. Badge images were not being proxied, causing mixed content warnings as well as leaking the IP address of the user.	7.5	More Details
CVE-2020-8571	StorageGRID (formerly StorageGRID Webscale) versions 10.0.0 through 11.3 prior to 11.2.0.8 and 11.3.0.4 are susceptible to a vulnerability which allows an unauthenticated remote attacker to cause a Denial of Service (DoS).	7.5	More Details
CVE-2020-1863	Huawei USG6000V with versions V500R001C20SPC300, V500R003C00SPC100, and V500R005C00SPC100 have an out-of-bounds read vulnerability. Due to a logical flaw in a JSON parsing routine, a remote, unauthenticated attacker could exploit this vulnerability to disrupt service in the affected products.	7.5	More Details
CVE-2015-3641	bitcoind and Bitcoin-Qt prior to 0.10.2 allow attackers to cause a denial of service (disabled functionality such as a client application crash) via an "Easy" attack.	7.5	More Details
CVE-2020-0876	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'.	7.5	More Details
CVE-2019-20191	Oxygen XML Editor 21.1.1 allows XXE to read any file.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10532	The AD Helper component in WatchGuard Fireware before 5.8.5.10317 allows remote attackers to discover cleartext passwords via the /domains/list URI.	7.5	More Details
CVE-2020-0847	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'.	7.5	More Details
CVE-2019-14303	Ricoh SP C250DN 1.05 devices allow denial of service (issue 1 of 3). Some Ricoh printers were affected by a wrong LPD service implementation that lead to a denial of service vulnerability.	7.5	More Details
CVE-2019-14309	Ricoh SP C250DN 1.05 devices have a fixed password. FTP service credential were found to be hardcoded within the printer firmware. This would allow to an attacker to access and read information stored on the shared FTP folders.	7.5	More Details
CVE-2020-0826	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0768, CVE-2020-0823, CVE-2020-0825, CVE-2020-0827, CVE-2020-0828, CVE-2020-0829, CVE-2020-0830, CVE-2020-0831, CVE-2020-0832, CVE-2020-0833, CVE-2020-0848.	7.5	More Details
CVE-2020-10591	An issue was discovered in Walmart Labs Concord before 1.44.0. CORS Access-Control-Allow-Origin headers have a potentially unsafe dependency on Origin headers, and are not configurable. This allows remote attackers to discover host information, nodes, API metadata, and references to usernames via api/v1/apikey.	7.5	More Details
CVE-2020-0815	An elevation of privilege vulnerability exists when Azure DevOps Server and Team Foundation Services improperly handle pipeline job tokens, aka 'Azure DevOps Server and Team Foundation Services Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0758.	7.5	More Details
CVE-2020-7919	Go before 1.12.16 and 1.13.x before 1.13.7 (and the crypto/cryptobyte package before 0.0.0-20200124225646-8b5121be2f68 for Go) allows attacks on clients (resulting in a panic) via a malformed X.509 certificate.	7.5	More Details
CVE-2020-0823	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0768, CVE-2020-0825, CVE-2020-0826, CVE-2020-0827, CVE-2020-0828, CVE-2020-0829, CVE-2020-0830, CVE-2020-0831, CVE-2020-0832, CVE-2020-0833, CVE-2020-0848.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0824	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'.	7.5	More Details
CVE-2020-0825	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0768, CVE-2020-0823, CVE-2020-0826, CVE-2020-0827, CVE-2020-0828, CVE-2020-0829, CVE-2020-0830, CVE-2020-0831, CVE-2020-0832, CVE-2020-0833, CVE-2020-0848.	7.5	More Details
CVE-2020-0827	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0768, CVE-2020-0823, CVE-2020-0825, CVE-2020-0826, CVE-2020-0828, CVE-2020-0829, CVE-2020-0830, CVE-2020-0831, CVE-2020-0832, CVE-2020-0833, CVE-2020-0848.	7.5	More Details
CVE-2019-19611	An issue was discovered in Halvotec RaQuest 10.23.10801.0. One of the exposed web services allows an anonymous user to access the list of connected users as well as the session cookie for each user. Fixed in Release 10.24.11206.1	7.5	More Details
CVE-2020-0828	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0768, CVE-2020-0823, CVE-2020-0825, CVE-2020-0826, CVE-2020-0827, CVE-2020-0829, CVE-2020-0830, CVE-2020-0831, CVE-2020-0832, CVE-2020-0833, CVE-2020-0848.	7.5	More Details
CVE-2020-10573	An issue was discovered in Janus through 0.9.1. janus_audiobridge.c has a double mutex unlock when listing private rooms in AudioBridge.	7.5	More Details
CVE-2020-0829	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0768, CVE-2020-0823, CVE-2020-0825, CVE-2020-0826, CVE-2020-0827, CVE-2020-0828, CVE-2020-0830, CVE-2020-0831, CVE-2020-0832, CVE-2020-0833, CVE-2020-0848.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0830	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0768, CVE-2020-0823, CVE-2020-0825, CVE-2020-0826, CVE-2020-0827, CVE-2020-0828, CVE-2020-0829, CVE-2020-0831, CVE-2020-0832, CVE-2020-0833, CVE-2020-0848.	7.5	More Details
CVE-2020-0832	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0768, CVE-2020-0823, CVE-2020-0825, CVE-2020-0826, CVE-2020-0827, CVE-2020-0828, CVE-2020-0829, CVE-2020-0830, CVE-2020-0831, CVE-2020-0833, CVE-2020-0848.	7.5	More Details
CVE-2020-0833	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0768, CVE-2020-0823, CVE-2020-0825, CVE-2020-0826, CVE-2020-0827, CVE-2020-0828, CVE-2020-0829, CVE-2020-0830, CVE-2020-0831, CVE-2020-0832, CVE-2020-0848.	7.5	More Details
CVE-2020-7248	libubox in OpenWrt before 18.06.7 and 19.x before 19.07.1 has a tagged binary data JSON serialization vulnerability that may cause a stack based buffer overflow.	7.5	More Details
CVE-2020-0831	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0768, CVE-2020-0823, CVE-2020-0825, CVE-2020-0826, CVE-2020-0827, CVE-2020-0828, CVE-2020-0829, CVE-2020-0830, CVE-2020-0832, CVE-2020-0833, CVE-2020-0848.	7.5	More Details
CVE-2019-5134	An exploitable regular expression without anchors vulnerability exists in the Web-Based Management (WBM) authentication functionality of WAGO PFC200 versions 03.00.39(12) and 03.01.07(13), and WAGO PFC100 version 03.00.39(12). A specially crafted authentication request can bypass regular expression filters, resulting in sensitive information disclosure.	7.5	More Details
CVE-2019-9098	An issue was discovered on Moxa MGate MB3170 and MB3270 devices before 4.1, MB3280 and MB3480 devices before 3.1, MB3660 devices before 2.3, and MB3180 devices before 2.1. An Integer overflow in the built-in web server allows remote attackers to initiate DoS.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-5149	The WBM web application on firmwares prior to 03.02.02 and 03.01.07 on the WAGO PFC100 and PFC2000, respectively, runs on a lighttpd web server and makes use of the FastCGI module, which is intended to provide high performance for all Internet applications without the penalties of Web server APIs. However, the default configuration of this module appears to limit the number of concurrent php-cgi processes to two, which can be abused to cause a denial of service of the entire web server. This affects WAGO PFC200 Firmware version 03.00.39(12) and version 03.01.07(13), and WAGO PFC100 Firmware version 03.00.39(12) and version 03.02.02(14).	7.5	More Details
CVE-2019-9101	An issue was discovered on Moxa MGate MB3170 and MB3270 devices before 4.1, MB3280 and MB3480 devices before 3.1, MB3660 devices before 2.3, and MB3180 devices before 2.1. Sensitive information is sent to the web server in cleartext, which may allow an attacker to discover the credentials if they are able to observe traffic between the web browser and the server.	7.5	More Details
CVE-2020-9435	PHOENIX CONTACT TC ROUTER 3002T-4G through 2.05.3, TC ROUTER 2002T-3G through 2.05.3, TC ROUTER 3002T-4G VZW through 2.05.3, TC ROUTER 3002T-4G ATT through 2.05.3, TC CLOUD CLIENT 1002-4G through 2.03.17, and TC CLOUD CLIENT 1002-TXTX through 1.03.17 devices contain a hardcoded certificate (and key) that is used by default for web-based services on the device. Impersonation, man-in-the-middle, or passive decryption attacks are possible if the generic certificate is not replaced by a device-specific certificate during installation.	7.5	More Details
CVE-2020-9464	A Denial-of-Service vulnerability exists in BECKHOFF Ethernet TCP/IP Bus Coupler BK9000. After an attack has occurred, the device's functionality can be restored by rebooting.	7.5	More Details
CVE-2020-0645	A tampering vulnerability exists when Microsoft IIS Server improperly handles malformed request headers, aka 'Microsoft IIS Server Tampering Vulnerability'.	7.5	More Details
CVE-2020-0758	An elevation of privilege vulnerability exists when Azure DevOps Server and Team Foundation Services improperly handle pipeline job tokens, aka 'Azure DevOps Server and Team Foundation Services Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0815.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7943	Puppet Server and PuppetDB provide useful performance and debugging information via their metrics API endpoints. For PuppetDB this may contain things like hostnames. Puppet Server reports resource names and titles for defined types (which may contain sensitive information) as well as function names and class names. Previously, these endpoints were open to the local network. PE 2018.1.13 & 2019.5.0, Puppet Server 6.9.2 & 5.3.12, and PuppetDB 6.9.1 & 5.2.13 disable trapperkeeper-metrics /v1 metrics API and only allows /v2 access on localhost by default. This affects software versions: Puppet Enterprise 2018.1.x stream prior to 2018.1.13 Puppet Enterprise prior to 2019.5.0 Puppet Server prior to 6.9.2 Puppet Server prior to 5.3.12 PuppetDB prior to 6.9.1 PuppetDB prior to 5.2.13 Resolved in: Puppet Enterprise 2018.1.13 Puppet Enterprise 2019.5.0 Puppet Server 6.9.2 Puppet Server 5.3.12 PuppetDB 6.9.1 PuppetDB 5.2.13	7.5	More Details
CVE-2019-9104	An issue was discovered on Moxa MGate MB3170 and MB3270 devices before 4.1, MB3280 and MB3480 devices before 3.1, MB3660 devices before 2.3, and MB3180 devices before 2.1. The application's configuration file contains parameters that represent passwords in cleartext.	7.5	More Details
CVE-2020-0768	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0823, CVE-2020-0825, CVE-2020-0826, CVE-2020-0827, CVE-2020-0828, CVE-2020-0829, CVE-2020-0830, CVE-2020-0831, CVE-2020-0832, CVE-2020-0833, CVE-2020-0848.	7.5	More Details
CVE-2013-1753	The gzip_decode function in the xmlrpc client library in Python 3.4 and earlier allows remote attackers to cause a denial of service (memory consumption) via a crafted HTTP request.	7.5	More Details
CVE-2019-5107	A cleartext transmission vulnerability exists in the network communication functionality of WAGO e!Cockpit version 1.5.1.1. An attacker with access to network traffic can easily intercept, interpret, and manipulate data coming from, or destined for e!Cockpit. This includes passwords, configurations, and binaries being transferred to endpoints.	7.5	More Details
CVE-2020-8787	SuiteCRM 7.10.x versions prior to 7.10.23 and 7.11.x versions prior to 7.11.11 allow for an invalid Bean ID to be submitted.	7.5	More Details
CVE-2019-10091	When TLS is enabled with ssl-endpoint-identification-enabled set to true, Apache Geode fails to perform hostname verification of the entries in the certificate SAN during the SSL handshake. This could compromise intra-cluster communication using a man-in-the-middle attack.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19135	In OPC Foundation OPC UA .NET Standard codebase 1.4.357.28, servers do not create sufficiently random numbers in OPCFoundation.NetStandard.Opc.Ua before 1.4.359.31, which allows man in the middle attackers to reuse encrypted user credentials sent over the network.	7.4	More Details
CVE-2019-2216	In overlay notifications, there is a possible hidden notification due to improper input validation. This could lead to a local escalation of privilege because the user is not notified of an overlaying app, with User execution privileges needed. User interaction is needed for exploitation.Product: Android Versions: Android-10 Android ID: A-38390530	7.3	More Details
CVE-2020-6581	Nagios NRPE 3.2.1 has Insufficient Filtering because, for example, nasty_metachars interprets \n as the character \ and the character n (not as the \n newline sequence). This can cause command injection.	7.3	More Details
CVE-2020-10390	OS Command Injection in export.php (vulnerable function called from include/functions-article.php) in Chadha PHPKB Standard Multi-Language 9 allows remote attackers to achieve Code Execution by saving the code to be executed as the wkhtmltopdf path via admin/save-settings.php.	7.2	More Details
CVE-2020-10562	An issue was discovered in DEVOME GRR before 3.4.1c. admin_edit_room.php mishandles file uploads.	7.2	More Details
CVE-2019-19937	In JFrog Artifactory before 6.18, it is not possible to restrict either system or repository imports by any admin user in the enterprise, which can lead to "undesirable results."	7.2	More Details
CVE-2019-19940	Incorrect input sanitation in text-oriented user interfaces (telnet, ssh) in Swisscom Centro Grande before 6.16.12 allows remote authenticated users to execute arbitrary commands via command injection.	7.2	More Details
CVE-2019-5155	An exploitable command injection vulnerability exists in the cloud connectivity feature of WAGO PFC200. An attacker can inject operating system commands into any of the parameter values contained in the firmware update command. This affects WAGO PFC200 Firmware version 03.02.02(14), version 03.01.07(13), and version 03.00.39(12)	7.2	More Details
CVE-2019-5156	An exploitable command injection vulnerability exists in the cloud connectivity functionality of WAGO PFC200 versions 03.02.02(14), 03.01.07(13), and 03.00.39(12). An attacker can inject operating system commands into the TimeoutPrepared parameter value contained in the firmware update command.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10120	cPanel before 84.0.20 allows resellers to achieve remote code execution as root via a cpsrvd rsync shell (SEC-545).	7.2	More Details
CVE-2019-5157	An exploitable command injection vulnerability exists in the Cloud Connectivity functionality of WAGO PFC200 Firmware versions 03.02.02(14), 03.01.07(13), and 03.00.39(12). An attacker can inject OS commands into the TimeoutUnconfirmed parameter value contained in the Firmware Update command.	7.2	More Details
CVE-2020-10115	cPanel before 84.0.20, when PowerDNS is used, allows arbitrary code execution as root via dnsadmin. (SEC-537).	7.2	More Details
CVE-2019-11355	An issue was discovered in Poly (formerly Polycom) HDX 3.1.13. A feature exists that allows the creation of a server / client certificate, or the upload of the user certificate, on the administrator's page. The value received from the user is the factor value of a shell script on the equipment. By entering a special character (such as a single quote) in a CN or other CSR field, one can insert a command into a factor value. A system command can be executed as root.	7.2	More Details
CVE-2020-5844	index.php?sec=godmode/extensions&sec2=extensions/files_repo in Pandora FMS v7.0 NG allows authenticated administrators to upload malicious PHP scripts, and execute them via base64 decoding of the file location. This affects v7.0NG.742_FIX_PERL2020.	7.2	More Details
CVE-2019-11073	A Remote Code Execution vulnerability exists in PRTG Network Monitor before 19.4.54.1506 that allows attackers to execute code due to insufficient sanitization when passing arguments to the HttpTransactionSensor.exe binary. In order to exploit the vulnerability, remote authenticated administrators need to create a new HTTP Transaction Sensor and set specific settings when the sensor is executed.	7.2	More Details
CVE-2019-19538	In Sangoma FreePBX 13 through 15 and sysadmin (aka System Admin) 13.0.92 through 15.0.13.6 modules have a Remote Command Execution vulnerability that results in Privilege Escalation.	7.2	More Details
CVE-2019-11074	A Write to Arbitrary Location in Disk vulnerability exists in PRTG Network Monitor 19.1.49 and below that allows attackers to place files in arbitrary locations with SYSTEM privileges (although not controlling the contents of such files) due to insufficient sanitisation when passing arguments to the phantomjs.exe binary. In order to exploit the vulnerability, remote authenticated administrators need to create a new HTTP Full Web Page Sensor and set specific settings when executing the sensor.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10386	admin/imagepaster/image-upload.php in Chadha PHPKB Standard Multi-Language 9 allows remote attackers to achieve Code Execution by uploading a .php file in the admin/js/ directory.	7.2	More Details
CVE-2020-10389	admin/save-settings.php in Chadha PHPKB Standard Multi-Language 9 allows remote attackers to achieve Code Execution by injecting PHP code into any POST parameter when saving global settings.	7.2	More Details
CVE-2020-0786	A denial of service vulnerability exists when the Windows Tile Object Service improperly handles hard links, aka 'Windows Tile Object Service Denial of Service Vulnerability'.	7.1	More Details
CVE-2020-0854	An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability'.	7.1	More Details
CVE-2020-0789	A denial of service vulnerability exists when the Visual Studio Extension Installer Service improperly handles hard links, aka 'Visual Studio Extension Installer Service Denial of Service Vulnerability'.	7.1	More Details
CVE-2020-0556	Improper access control in subsystem for BlueZ before version 5.54 may allow an unauthenticated user to potentially enable escalation of privilege and denial of service via adjacent access	7.1	More Details
CVE-2020-0785	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'.	7.1	More Details
CVE-2020-1981	A predictable temporary filename vulnerability in PAN-OS allows local privilege escalation. This issue allows a local attacker who bypassed the restricted shell to execute commands as a low privileged user and gain root access on the PAN-OS hardware or virtual appliance. This issue affects only PAN-OS 8.1 versions earlier than PAN-OS 8.1.13. This issue does not affect PAN-OS 7.1, PAN-OS 9.0, or later PAN-OS versions.	7.0	More Details
CVE-2019-14626	Improper access control in PCIe function for the Intel® FPGA Programmable Acceleration Card N3000, all versions, may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2019-15708	A system command injection vulnerability in the FortiAP-S/W2 6.2.1, 6.2.0, 6.0.5 and below, FortiAP 6.0.5 and below and FortiAP-U below 6.0.0 under CLI admin console may allow unauthorized administrators to run arbitrary system level commands via specially crafted ifconfig commands.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-18576	Dell EMC XtremIO XMS versions prior to 6.3.0 contain an information disclosure vulnerability where OS users' passwords are logged in local files. Malicious local users with access to the log files may use the exposed passwords to gain access to XtremIO with the privileges of the compromised user.	6.7	More Details
CVE-2019-18577	Dell EMC XtremIO XMS versions prior to 6.3.0 contain an incorrect permission assignment vulnerability. A malicious local user with XtremIO xinstall privileges may exploit this vulnerability to gain root access.	6.7	More Details
CVE-2020-0526	Improper input validation in firmware for Intel(R) NUC may allow a privileged user to potentially enable escalation of privilege via local access. The list of affected products is provided in intel-sa-00343: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00343.html	6.7	More Details
CVE-2019-4656	IBM MQ and IBM MQ Appliance 7.1, 7.5, 8.0, 9.0 LTS, 9.1 LTS, and 9.1 CD is vulnerable to a denial of service attack that would allow an authenticated user to crash the queue and require a restart due to an error processing error messages. IBM X-Force ID: 170967.	6.5	More Details
CVE-2020-10081	GitLab before 12.8.2 has Incorrect Access Control. It was internally discovered that the LFS import process could potentially be used to incorrectly access LFS objects not owned by the user.	6.5	More Details
CVE-2020-6858	Hotels Styx through 1.0.0.beta8 allows HTTP response splitting due to CRLF Injection. This is exploitable if untrusted user input can appear in a response header.	6.5	More Details
CVE-2020-10501	CSRF in admin/manage-departments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to edit a department, given the id, via a crafted request.	6.5	More Details
CVE-2020-7916	be_teacher in class-lp-admin-ajax.php in the LearnPress plugin 3.2.6.5 and earlier for WordPress allows any registered user to assign itself the teacher role via the wp-admin/admin-ajax.php?action=learnpress_be_teacher URI without any additional permission checks. Therefore, any user can change its role to an instructor/teacher and gain access to otherwise restricted data.	6.5	More Details
CVE-2019-13170	Some Xerox printers (such as the Phaser 3320 V53.006.16.000) did not implement any mechanism to avoid CSRF attacks. Successful exploitation of this vulnerability can lead to the takeover of a local account on the device.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10498	CSRF in admin/edit-category.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to edit a category, given the id, via a crafted request.	6.5	More Details
CVE-2020-10497	CSRF in admin/manage-categories.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete a category via a crafted request.	6.5	More Details
CVE-2019-2058	In libAACdec, there is a possible out of bounds read. This could lead to remote information disclosure, with no additional execution privileges needed. User interaction is needed for exploitation.Product: Android Versions: Android-10 Android ID: A-136089102	6.5	More Details
CVE-2020-0882	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0774, CVE-2020-0874, CVE-2020-0879, CVE-2020-0880.	6.5	More Details
CVE-2020-0880	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0774, CVE-2020-0874, CVE-2020-0879, CVE-2020-0882.	6.5	More Details
CVE-2019-5648	Authenticated, administrative access to a Barracuda Load Balancer ADC running unpatched firmware <= v6.4 allows one to edit the LDAP service configuration of the balancer and change the LDAP server to an attacker-controlled system, without having to re-enter LDAP credentials. These steps can be used by any authenticated administrative user to expose the LDAP credentials configured in the LDAP connector over the network.	6.5	More Details
CVE-2020-10218	A Blind SQL Injection issue was discovered in Sapplica Sentrifugo 3.2 via the index.php/holidaygroups/add id parameter because of the HolidaydatesController.php addAction function.	6.5	More Details
CVE-2020-0088	In parseTrackFragmentRun of MPEG4Extractor.cpp, there is possible resource exhaustion due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-124389881	6.5	More Details
CVE-2019-20495	cPanel before 82.0.18 allows attackers to read an arbitrary database via MySQL dump streaming (SEC-531).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-13199	Some Kyocera printers (such as the ECOSYS M5526cdw 2R7_2000.001.701) did not implement any mechanism to avoid CSRF. Successful exploitation of this vulnerability can lead to the takeover of a local account on the device.	6.5	More Details
CVE-2020-10122	cPanel before 84.0.20 allows a webmail or demo account to delete arbitrary files (SEC-547).	6.5	More Details
CVE-2020-0853	An information disclosure vulnerability exists in Windows when the Windows Imaging Component fails to properly handle objects in memory, aka 'Windows Imaging Component Information Disclosure Vulnerability'.	6.5	More Details
CVE-2019-18917	A potential security vulnerability has been identified for certain HP Printers and All-in-Ones that would allow bypassing account lockout.	6.5	More Details
CVE-2018-13060	Easy!Appointments 1.3.0 has a Guessable CAPTCHA issue.	6.5	More Details
CVE-2019-16157	An information exposure vulnerability in Fortinet FortiWeb 6.2.0 CLI and earlier may allow an authenticated user to view sensitive information being logged via diagnose debug commands.	6.5	More Details
CVE-2020-6584	Nagios Log Server 2.1.3 has Incorrect Access Control.	6.5	More Details
CVE-2020-10458	Path Traversal in admin/imagepaster/operations.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete any folder on the webserver using a dot-dot-slash sequence (../) via the GET parameter crdir, when the GET parameter action is set to df, causing a Denial of Service.	6.5	More Details
CVE-2019-19946	The API in Dradis Pro 3.4.1 allows any user to extract the content of a project, even if this user is not part of the project team.	6.5	More Details
CVE-2020-0774	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0874, CVE-2020-0879, CVE-2020-0880, CVE-2020-0882.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9472	Umbraco CMS 8.5.3 allows an authenticated file upload (and consequently Remote Code Execution) via the Install Package functionality.	6.5	More Details
CVE-2019-3769	Dell Wyse Management Suite versions prior to 1.4.1 contain a stored cross-site scripting vulnerability. A remote authenticated malicious user with low privileges could exploit this vulnerability to store malicious payload in the device heartbeat request. When victim users access the submitted data through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application.	6.4	More Details
CVE-2019-3770	Dell Wyse Management Suite versions prior to 1.4.1 contain a stored cross-site scripting vulnerability when unregistering a device. A remote authenticated malicious user with low privileges could exploit this vulnerability to store malicious HTML or JavaScript code. When victim users access the submitted data through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application.	6.4	More Details
CVE-2020-10195	The popup-builder plugin before 3.64.1 for WordPress allows information disclosure and settings modification, leading to in-scope privilege escalation via admin-post actions to com/classes/Actions.php. By sending a POST request to wp-admin/admin-post.php, an authenticated attacker with minimal (subscriber-level) permissions can modify the plugin's settings to allow arbitrary roles (including subscribers) access to plugin functionality by setting the action parameter to sgpbSaveSettings, export a list of current newsletter subscribers by setting the action parameter to csv_file, or obtain system configuration information including webserver configuration and a list of installed plugins by setting the action parameter to sgpb_system_info.	6.3	More Details
CVE-2020-10196	An XSS vulnerability in the popup-builder plugin before 3.64.1 for WordPress allows remote attackers to inject arbitrary JavaScript into existing popups via an unsecured ajax action in com/classes/Ajax.php. It is possible for an unauthenticated attacker to insert malicious JavaScript in several of the popup's fields by sending a request to wp-admin/admin-ajax.php with the POST action parameter of sgpb_autosave and including additional data in an allPopupData parameter, including the popup's ID (which is visible in the source of the page in which the popup is inserted) and arbitrary JavaScript which will then be executed in the browsers of visitors to that page. Because the plugin functionality automatically adds script tags to data entered into these fields, this injection will typically bypass most WAF applications.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-13167	Multiple Stored XSS vulnerabilities were found in the Xerox Web Application, used by the Phaser 3320 V53.006.16.000 and other printers. Successful exploitation of this vulnerability can lead to session hijacking of the administrator in the web application or the execution of unwanted actions.	6.1	More Details
CVE-2020-10544	An XSS issue was discovered in tooltip/tooltip.js in PrimeTek PrimeFaces 7.0.11. In a web application using PrimeFaces, an attacker can provide JavaScript code in an input field whose data is later used as a tooltip title without any input validation.	6.1	More Details
CVE-2009-5159	Invision Power Board (aka IPB or IP.Board) 2.x through 3.0.4, when Internet Explorer 5 is used, allows XSS via a .txt attachment.	6.1	More Details
CVE-2020-10076	GitLab 12.1 through 12.8.1 allows XSS. A stored cross-site scripting vulnerability was discovered when displaying merge requests.	6.1	More Details
CVE-2020-10075	GitLab 12.5 through 12.8.1 allows HTML Injection. A particular error header was potentially susceptible to injection or potentially other vulnerabilities via unescaped input.	6.1	More Details
CVE-2019-16156	An Improper Neutralization of Input vulnerability in the Anomaly Detection Parameter Name in Fortinet FortiWeb 6.0.5, 6.2.0, and 6.1.1 may allow a remote unauthenticated attacker to perform a Cross Site Scripting attack (XSS).	6.1	More Details
CVE-2020-0505	Improper conditions check in Intel(R) Graphics Drivers before versions 15.33.49.5100, 15.36.38.5117, 15.40.44.5107, 15.45.30.5103, and 26.20.100.7212 may allow an authenticated user to potentially enable information disclosure and denial of service via local	6.1	More Details
CVE-2019-13198	The web application of several Kyocera printers (such as the ECOSYS M5526cdw 2R7_2000.001.701) was affected by Stored XSS. Successful exploitation of this vulnerability can lead to session hijacking of the administrator in the web application or the execution of unwanted actions.	6.1	More Details
CVE-2018-10704	yidashi yii2cmf 2.0 has XSS via the /search q parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-13200	The web application of several Kyocera printers (such as the ECOSYS M5526cdw 2R7_2000.001.701) was affected by Reflected XSS. Successful exploitation of this vulnerability can lead to session hijacking of the administrator in the web application or the execution of unwanted actions.	6.1	More Details
CVE-2020-10091	GitLab 9.3 through 12.8.1 allows XSS. A cross-site scripting vulnerability was found when viewing particular file types.	6.1	More Details
CVE-2020-10078	GitLab 12.1 through 12.8.1 allows XSS. The merge request submission form was determined to have a stored cross-site scripting vulnerability.	6.1	More Details
CVE-2020-10092	GitLab 12.1 through 12.8.1 allows XSS. A cross-site scripting vulnerability was present in a particular view relating to the Grafana integration.	6.1	More Details
CVE-2019-19381	oauth/oauth2/v1/saml/ in Abacus OAuth Login 2019_01_r4_20191021_0000 before prior to R4 (20.11.2019 Hotfix) allows Reflected Cross Site Scripting (XSS) via an error message.	6.1	More Details
CVE-2020-8436	XSS was discovered in the RegistrationMagic plugin 4.6.0.0 for WordPress via the rm_form_id, rm_tr, or form_name parameter.	6.1	More Details
CVE-2019-6696	An improper input validation vulnerability in FortiOS 6.2.1, 6.2.0, 6.0.8 and below until 5.4.0 under admin webUI may allow an attacker to perform an URL redirect attack via a specifically crafted request to the admin initial password change webpage.	6.1	More Details
CVE-2020-10242	An issue was discovered in Joomla! before 3.9.16. Inadequate handling of CSS selectors in the Protostar and Beez3 JavaScript allows XSS attacks.	6.1	More Details
CVE-2019-19211	Dolibarr ERP/CRM before 10.0.3 has an Insufficient Filtering issue that can lead to user/card.php XSS.	6.1	More Details
CVE-2020-10461	The way comments in article.php (vulnerable function in include/functions-article.php) are handled in Chadha PHPKB Standard Multi-Language 9 allows attackers to execute Stored (Blind) XSS (injecting arbitrary web script or HTML) in admin/manage-comments.php, via the GET parameter cmt.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14512	LimeSurvey 3.17.7+190627 has XSS via Boxes in application/extensions/PanelBoxWidget/views/box.php or a label title in application/views/admin/labels/labelview_view.php.	6.1	More Details
CVE-2018-10125	Contao before 4.5.7 has XSS in the system log.	6.1	More Details
CVE-2020-10113	cPanel before 84.0.20 allows self XSS via a temporary character-set specification (SEC-515).	6.1	More Details
CVE-2020-10114	cPanel before 84.0.20 allows stored self-XSS via the HTML file editor (SEC-535).	6.1	More Details
CVE-2019-20493	cPanel before 82.0.18 allows self-XSS because JSON string escaping is mishandled (SEC-520).	6.1	More Details
CVE-2011-2487	The implementations of PKCS#1 v1.5 key transport mechanism for XMLEncryption in JBossWS and Apache WSS4J before 1.6.5 is susceptible to a Bleichenbacher attack.	5.9	More Details
CVE-2019-15608	The package integrity validation in yarn < 1.19.0 contains a TOCTOU vulnerability where the hash is computed before writing a package to cache. It's not computed again when reading from the cache. This may lead to a cache pollution attack.	5.9	More Details
CVE-2017-18350	bitcoind and Bitcoin-Qt prior to 0.15.1 have a stack-based buffer overflow if an attacker-controlled SOCKS proxy server is used. This results from an integer signedness error when the proxy server responds with an acknowledgement of an unexpected target domain name.	5.9	More Details
CVE-2020-0574	Improper configuration in block design for Intel(R) MAX(R) 10 FPGA all versions may allow an authenticated user to potentially enable escalation of privilege and information disclosure via physical access.	5.9	More Details
CVE-2020-6175	Citrix SD-WAN 10.2.x before 10.2.6 and 11.0.x before 11.0.3 has Missing SSL Certificate Validation.	5.9	More Details
CVE-2020-10576	An issue was discovered in Janus through 0.9.1. plugins/janus_voicemail.c in the VoiceMail plugin has a race condition that could cause a server crash.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7253	Improper access control vulnerability in masvc.exe in McAfee Agent (MA) prior to 5.6.4 allows local users with administrator privileges to disable self-protection via a McAfee supplied command-line utility.	5.7	More Details
CVE-2020-7598	minimist before 1.2.2 could be tricked into adding or modifying properties of Object.prototype using a "constructor" or "__proto__" payload.	5.6	More Details
CVE-2020-0551	Load value injection in some Intel(R) Processors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. The list of affected products is provided in intel-sa-00334: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00334.html	5.6	More Details
CVE-2020-0550	Improper data forwarding in some data cache for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. The list of affected products is provided in intel-sa-00330: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00330.html	5.6	More Details
CVE-2019-4619	IBM MQ and IBM MQ Appliance 7.1, 7.5, 8.0, 9.0 LTS, 9.1 LTS, and 9.1 CD could allow a local attacker to obtain sensitive information by inclusion of sensitive data within trace. IBM X-Force ID: 168862.	5.5	More Details
CVE-2019-2088	In StatsService, there is a possible out of bounds read. This could lead to local information disclosure if UBSAN were not enabled, with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-10 Android ID: A-143895055	5.5	More Details
CVE-2012-1101	systemd 37-1 does not properly handle non-existent services, which causes a denial of service (failure of login procedure).	5.5	More Details
CVE-2019-5106	A hard-coded encryption key vulnerability exists in the authentication functionality of WAGO e!Cockpit version 1.5.1.1. An attacker with access to communications between e!Cockpit and CoDeSyS Gateway can trivially recover the password of any user attempting to log in, in plain text.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-5177	An exploitable stack buffer overflow vulnerability vulnerability exists in the iocheckd service ‘I/O-Check’ functionality of WAGO PFC 200 Firmware version 03.02.02(14). The destination buffer sp+0x440 is overflowed with the call to sprintf() for any domainname values that are greater than 1024-len(‘/etc/config-tools/edit_dns_server domain-name=‘) in length. A domainname value of length 0x3fa will cause the service to crash.	5.5	More Details
CVE-2020-0567	Improper input validation in Intel(R) Graphics Drivers before version 26.20.100.7212 may allow an authenticated user to enable denial of service via local access.	5.5	More Details
CVE-2019-5182	An exploitable stack buffer overflow vulnerability vulnerability exists in the iocheckd service ‘I/O-Check’ functionality of WAGO PFC 200 Firmware version 03.02.02(14). An attacker can send a specially crafted packet to trigger the parsing of this cache file.The destination buffer sp+0x440 is overflowed with the call to sprintf() for any type values that are greater than 1024-len(‘/etc/config-tools/config_interfaces interface=X1 state=enabled config-type=‘) in length. A type value of length 0x3d9 will cause the service to crash.	5.5	More Details
CVE-2019-5176	An exploitable stack buffer overflow vulnerability vulnerability exists in the iocheckd service ‘I/O-Check’ functionality of WAGO PFC 200 Firmware version 03.02.02(14). An attacker can send a specially crafted packet to trigger the parsing of this cache file.The destination buffer sp+0x40 is overflowed with the call to sprintf() for any gateway values that are greater than 512-len(‘/etc/config-tools/config_default_gateway number=0 state=enabled value=‘) in length. A gateway value of length 0x7e2 will cause the service to crash.	5.5	More Details
CVE-2019-4719	IBM MQ and IBM MQ Appliance 7.1, 7.5, 8.0, 9.0 LTS, 9.1 LTS, and 9.1 CD could allow a local attacker to obtain sensitive information by inclusion of sensitive data within runmqras data.	5.5	More Details
CVE-2020-9064	Huawei smartphone Honor V30 with versions earlier than OxfordS-AN00A 10.0.1.167(C00E166R4P1) have an improper authentication vulnerability. Authentication to target component is improper when device performs an operation. Attackers exploit this vulnerability to obtain some information by loading malicious application, leading to information leak.	5.5	More Details
CVE-2020-0859	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Service Information Disclosure Vulnerability'.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0874	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0774, CVE-2020-0879, CVE-2020-0880, CVE-2020-0882.	5.5	More Details
CVE-2020-0879	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0774, CVE-2020-0874, CVE-2020-0880, CVE-2020-0882.	5.5	More Details
CVE-2020-0511	Uncaught exception in system driver for Intel(R) Graphics Drivers before version 15.40.44.5107 may allow an authenticated user to potentially enable a denial of service via local access.	5.5	More Details
CVE-2020-0820	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-0871	An information disclosure vulnerability exists when Windows Network Connections Service fails to properly handle objects in memory, aka 'Windows Network Connections Service Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-0516	Improper access control in Intel(R) Graphics Drivers before version 26.20.100.7463 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2019-20496	cPanel before 82.0.18 allows attackers to conduct arbitrary chown operations as root during log processing (SEC-532).	5.5	More Details
CVE-2020-0765	An information disclosure vulnerability exists in the Remote Desktop Connection Manager (RDCMan) application when it improperly parses XML input containing a reference to an external entity, aka 'Remote Desktop Connection Manager Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-0503	Improper access control in Intel(R) Graphics Drivers before version 26.20.100.7212 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2020-5959	NVIDIA Virtual GPU Manager, all versions, contains a vulnerability in the vGPU plugin in which an input index value is incorrectly validated which may lead to denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5960	NVIDIA Virtual GPU Manager contains a vulnerability in the kernel module (nvidia.ko), where a null pointer dereference may occur, which may lead to denial of service.	5.5	More Details
CVE-2020-5961	NVIDIA vGPU graphics driver for guest OS contains a vulnerability in which an incorrect resource clean up on a failure path can impact the guest VM, leading to denial of service.	5.5	More Details
CVE-2020-0775	An information disclosure vulnerability exists when Windows Error Reporting improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Error Reporting Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-0863	An information vulnerability exists when Windows Connected User Experiences and Telemetry Service improperly discloses file information, aka 'Connected User Experiences and Telemetry Service Information Disclosure Vulnerability'.	5.5	More Details
CVE-2020-0779	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0798, CVE-2020-0814, CVE-2020-0842, CVE-2020-0843.	5.5	More Details
CVE-2020-0501	Buffer overflow in Intel(R) Graphics Drivers before version 26.20.100.6912 may allow an authenticated user to potentially enable a denial of service via local access.	5.5	More Details
CVE-2020-10596	OpenCart 3.0.3.2 allows remote authenticated users to conduct XSS attacks via a crafted filename in the users' image upload section.	5.4	More Details
CVE-2019-19610	An issue was discovered in Halvotec RaQuest 10.23.10801.0. It allows session fixation. Fixed in Release 24.2020.20608.0.	5.4	More Details
CVE-2019-19941	Missing hostname validation in Swisscom Centro Grande before 6.16.12 allows a remote attacker to inject its local IP address as a domain entry in the DNS service of the router via crafted hostnames in DHCP requests, causing XSS.	5.4	More Details
CVE-2020-10388	The way the Referer header in article.php is handled in Chadha PHPKB Standard Multi-Language 9 allows attackers to execute Stored (Blind) XSS (injecting arbitrary web script or HTML) in admin/report-referrers.php (vulnerable file admin/include/functions-articles.php).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0891	This vulnerability is caused when SharePoint Server does not properly sanitize a specially crafted request to an affected SharePoint server.An authenticated attacker could exploit this vulnerability by sending a specially crafted request to an affected SharePoint server, aka 'Microsoft SharePoint Reflective XSS Vulnerability'. This CVE ID is unique from CVE-2020-0795.	5.4	More Details
CVE-2019-19612	An issue was discovered in Halvotec RaQuest 10.23.10801.0. Several features of the application allow stored Cross-site Scripting (XSS). Fixed in Release 24.2020.20608.0.	5.4	More Details
CVE-2020-6586	Nagios Log Server 2.1.3 allows XSS by visiting /profile and entering a crafted name field that is mishandled on the /admin/users page. Any malicious user with limited access can store an XSS payload in his Name. When any admin views this, the XSS is triggered.	5.4	More Details
CVE-2019-19210	Dolibarr ERP/CRM before 10.0.3 allows XSS because uploaded HTML documents are served as text/html despite being renamed to .noexe files.	5.4	More Details
CVE-2020-0893	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0894.	5.4	More Details
CVE-2019-6699	An improper neutralization of input vulnerability in Fortinet FortiADC 5.3.3 and earlier may allow an attacker to execute a stored Cross Site Scripting (XSS) via a field in the traffic group interface.	5.4	More Details
CVE-2019-20491	cPanel before 82.0.18 allows attackers to leverage virtual mail accounts in order to bypass account suspensions (SEC-508).	5.4	More Details
CVE-2019-20497	cPanel before 82.0.18 allows stored XSS via WHM Backup Restoration (SEC-533).	5.4	More Details
CVE-2020-0894	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0893.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6646	An improper neutralization of input vulnerability in FortiWeb allows a remote authenticated attacker to perform a stored cross site scripting attack (XSS) via the Disclaimer Description of a Replacement Message.	5.4	More Details
CVE-2020-0700	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server does not properly sanitize user provided input, aka 'Azure DevOps Server Cross-site Scripting Vulnerability'.	5.4	More Details
CVE-2020-6643	An improper neutralization of input vulnerability in the URL Description in Fortinet FortiIsolator version 1.2.2 allows a remote authenticated attacker to perform a cross site scripting attack (XSS).	5.4	More Details
CVE-2020-0903	A cross-site-scripting (XSS) vulnerability exists when Microsoft Exchange Server does not properly sanitize a specially crafted web request to an affected Exchange server, aka 'Microsoft Exchange Server Spoofing Vulnerability'.	5.4	More Details
CVE-2020-0795	This vulnerability is caused when SharePoint Server does not properly sanitize a specially crafted request to an affected SharePoint server.An authenticated attacker could exploit this vulnerability by sending a specially crafted request to an affected SharePoint server, aka 'Microsoft SharePoint Reflective XSS Vulnerability'. This CVE ID is unique from CVE-2020-0891.	5.4	More Details
CVE-2019-19461	Post-authentication Stored XSS in Team Password Manager through 7.93.204 allows attackers to steal other users' credentials by creating a shared password with HTML code as the title.	5.4	More Details
CVE-2018-20586	bitcoind and Bitcoin-Qt prior to 0.17.1 allow injection of arbitrary data into the debug log via an RPC call.	5.3	More Details
CVE-2016-1000111	Twisted before 16.3.1 does not attempt to address RFC 3875 section 4.1.18 namespace conflicts and therefore does not protect CGI applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect a CGI application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue.	5.3	More Details
CVE-2020-9519	HTTP methods reveled in Web services vulnerability in Micro Focus Service manager (server), affecting versions 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62, 9.63. The vulnerability could be exploited to allow exposure of configuration data.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9518	Login filter can access configuration files vulnerability in Micro Focus Service Manager (Web Tier), affecting versions 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. The vulnerability could be exploited to allow unauthorized access to configuration data.	5.3	More Details
CVE-2019-5135	An exploitable timing discrepancy vulnerability exists in the authentication functionality of the Web-Based Management (WBM) web application on WAGO PFC100/200 controllers. The WBM application makes use of the PHP crypt() function which can be exploited to disclose hashed user credentials. This affects WAGO PFC200 Firmware version 03.00.39(12) and version 03.01.07(13), and WAGO PFC100 Firmware version 03.00.39(12).	5.3	More Details
CVE-2020-10240	An issue was discovered in Joomla! before 3.9.16. Missing length checks in the user table can lead to the creation of users with duplicate usernames and/or email addresses.	5.3	More Details
CVE-2020-10116	cPanel before 84.0.20 allows attackers to bypass intended restrictions on features and demo accounts via WebDisk UAPI calls (SEC-541).	5.3	More Details
CVE-2019-9103	An issue was discovered on Moxa MGate MB3170 and MB3270 devices before 4.1, MB3280 and MB3480 devices before 3.1, MB3660 devices before 2.3, and MB3180 devices before 2.1. An attacker can access sensitive information (e.g., conduct username disclosure attacks) on the built-in WEB-service without authorization.	5.3	More Details
CVE-2018-18576	The Hustle (aka wordpress-popup) plugin through 6.0.5 for WordPress allows Directory Traversal to obtain a directory listing via the views/admin/dashboard/ URI.	5.3	More Details
CVE-2019-9097	An issue was discovered on Moxa MGate MB3170 and MB3270 devices before 4.1, MB3280 and MB3480 devices before 3.1, MB3660 devices before 2.3, and MB3180 devices before 2.1. A high rate of transit traffic may cause a low-memory condition and a denial of service.	5.3	More Details
CVE-2020-7608	yargs-parser could be tricked into adding or modifying properties of Object.prototype using a "__proto__" payload.	5.3	More Details
CVE-2020-0502	Improper access control in Intel(R) Graphics Drivers before version 26.20.100.6912 may allow an authenticated user to potentially enable escalation of privilege via local access.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7600	querymen prior to 2.1.4 allows modification of object properties. The parameters of exported function handler(type, name, fn) can be controlled by users without any sanitization. This could be abused for Prototype Pollution attacks.	5.3	More Details
CVE-2020-10082	GitLab 12.2 through 12.8.1 allows Denial of Service. A denial of service vulnerability impacting the designs for public issues was discovered.	5.3	More Details
CVE-2020-10535	GitLab 12.8.x before 12.8.6, when sign-up is enabled, allows remote attackers to bypass email domain restrictions within the two-day grace period for an unconfirmed email address.	5.3	More Details
CVE-2020-10084	GitLab EE 11.6 through 12.8.1 allows Information Disclosure. Sending a specially crafted request to the vulnerability_feedback endpoint could result in the exposure of a private project namespace	5.3	More Details
CVE-2018-19516	messagepartthemes/default/defaultrenderer.cpp in messagelib in KDE Applications before 18.12.0 does not properly restrict the handling of an http-equiv="REFRESH" value.	5.3	More Details
CVE-2020-10085	GitLab 12.3.5 through 12.8.1 allows Information Disclosure. A particular view was exposing merge private merge request titles.	5.3	More Details
CVE-2020-10080	GitLab 8.3 through 12.8.1 allows Information Disclosure. It was possible for certain non-members to access the Contribution Analytics page of a private group.	5.3	More Details
CVE-2020-10086	GitLab 10.4 through 12.8.1 allows Directory Traversal. A particular endpoint was vulnerable to a directory traversal vulnerability, leading to arbitrary file read.	5.3	More Details
CVE-2020-10079	GitLab 7.10 through 12.8.1 has Incorrect Access Control. Under certain conditions where users should have been required to configure two-factor authentication, it was not being required.	5.3	More Details
CVE-2019-19799	Zoho ManageEngine Applications Manager before 14600 allows a remote unauthenticated attacker to disclose license related information via WieldFeedServlet servlet.	5.3	More Details
CVE-2020-0517	Out-of-bounds write in Intel(R) Graphics Drivers before version 15.36.38.5117 may allow an authenticated user to potentially enable escalation of privilege or denial of service via local access.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10090	GitLab 11.7 through 12.8.1 allows Information Disclosure. Under certain group conditions, group epic information was unintentionally being disclosed.	5.3	More Details
CVE-2019-19613	An issue was discovered in Halvotec RaQuest 10.23.10801.0. The login page of the admin application is vulnerable to an Open Redirect attack allowing an attacker to redirect a user to a malicious site after authentication. The attacker needs to be on the same network to modify the victim's request on the wire. Fixed in Release 24.2020.20608.0	5.2	More Details
CVE-2020-1733	A race condition flaw was found in Ansible Engine 2.7.17 and prior, 2.8.9 and prior, 2.9.6 and prior when running a playbook with an unprivileged become user. When Ansible needs to run a module with become user, the temporary directory is created in /var/tmp. This directory is created with "umask 77 && mkdir -p <dir>"; this operation does not fail if the directory already exists and is owned by another user. An attacker could take advantage to gain control of the become user as the target directory can be retrieved by iterating '/proc/<pid>/cmdline'.	5.0	More Details
CVE-2020-1753	A security flaw was found in Ansible Engine, all Ansible 2.7.x versions prior to 2.7.17, all Ansible 2.8.x versions prior to 2.8.11 and all Ansible 2.9.x versions prior to 2.9.7, when managing kubernetes using the k8s module. Sensitive parameters such as passwords and tokens are passed to kubectl from the command line, not using an environment variable or an input configuration file. This will disclose passwords and tokens from process list and no_log directive from debug module would not have any effect making these secrets being disclosed on stdout and log files.	5.0	More Details
CVE-2020-10387	Path Traversal in admin/download.php in Chadha PHPKB Standard Multi-Language 9 allows remote attackers to download files from the server using a dot-dot-slash sequence (../) via the GET parameter file.	4.9	More Details
CVE-2020-10460	admin/include/operations.php (via admin/email-harvester.php) in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject untrusted input inside CSV files via the POST parameter data.	4.9	More Details
CVE-2019-20105	The EditApplinkServlet resource in the Atlassian Application Links plugin before version 5.4.20, from version 6.0.0 before version 6.0.12, from version 6.1.0 before version 6.1.2, from version 7.0.0 before version 7.0.1, and from version 7.1.0 before version 7.1.3 allows remote attackers who have obtained access to administrator's session to access the EditApplinkServlet resource without needing to re-authenticate to pass "WebSudo" in products that support "WebSudo" through an improper access control vulnerability.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19851	An XSS Injection vulnerability exists in Sangoma FreePBX and PBXact 13, 14, and 15 within the Debug/Test page of the Superfecta module at the admin/config.php?display=superfecta URI. This affects Superfecta through 13.0.4.7, 14.x through 14.0.24, and 15.x through 15.0.2.20.	4.8	More Details
CVE-2020-10470	Reflected XSS in admin/manage-fields.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.	4.8	More Details
CVE-2020-10469	Reflected XSS in admin/manage-departments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.	4.8	More Details
CVE-2020-10468	Reflected XSS in admin/edit-news.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter p.	4.8	More Details
CVE-2020-10467	Reflected XSS in admin/edit-comment.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter p.	4.8	More Details
CVE-2020-10427	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-languages.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10466	Reflected XSS in admin/edit-glossary.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter p.	4.8	More Details
CVE-2020-10420	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-comments.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10426	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-groups.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10432	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-tickets.php by adding a question mark (?) followed by the payload.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10464	Reflected XSS in admin/edit-article.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter p.	4.8	More Details
CVE-2020-10463	Reflected XSS in admin/edit-template.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter p.	4.8	More Details
CVE-2020-10425	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-glossary.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10462	Reflected XSS in admin/edit-field.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter p.	4.8	More Details
CVE-2020-10422	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-drafts.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10423	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-feedbacks.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10465	Reflected XSS in admin/edit-category.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter p.	4.8	More Details
CVE-2020-10421	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-departments.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10471	Reflected XSS in admin/manage-articles.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.	4.8	More Details
CVE-2020-10419	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-categories.php by adding a question mark (?) followed by the payload.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10418	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-attachments.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10417	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-articles.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10428	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-news.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10429	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-settings.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10477	Reflected XSS in admin/manage-news.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.	4.8	More Details
CVE-2020-10476	Reflected XSS in admin/manage-glossary.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.	4.8	More Details
CVE-2020-10416	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/kb-backup.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10430	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-subscribers.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10431	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-templates.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10475	Reflected XSS in admin/manage-tickets.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10474	Reflected XSS in admin/manage-comments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.	4.8	More Details
CVE-2020-10415	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/index.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10456	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/trash-box.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2019-19615	Multiple XSS vulnerabilities exist in the Backup & Restore module \ v14.0.10.2 through v14.0.10.7 for FreePBX, as shown at /admin/config.php?display=backup on the FreePBX Administrator web site. An attacker can modify the id parameter of the backup configuration screen and embed malicious XSS code via a link. When another user (such as an admin) clicks the link, the XSS payload will render and execute in the context of the victim user's account.	4.8	More Details
CVE-2019-19852	An XSS Injection vulnerability exists in Sangoma FreePBX and PBXact 13, 14, and 15 within the Call Event Logging report screen in the cel module at the admin/config.php?display=cel URI via date fields. This affects cel through 13.0.26.9, 14.x through 14.0.2.14, and 15.x through 15.0.15.4.	4.8	More Details
CVE-2020-10473	Reflected XSS in admin/manage-categories.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.	4.8	More Details
CVE-2020-10472	Reflected XSS in admin/manage-templates.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to inject arbitrary web script or HTML via the GET parameter sort.	4.8	More Details
CVE-2020-10433	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-users.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10407	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-news.php by adding a question mark (?) followed by the payload.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10455	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/translate.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10406	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-group.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10396	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-language.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10397	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-news.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10434	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-versions.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10435	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/my-languages.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10440	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-article-mailed.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10439	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-article-discussed.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10438	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/reply-ticket.php by adding a question mark (?) followed by the payload.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10398	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-template.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10399	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-user.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10400	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/article-collaboration.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10411	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/email-harvester.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10437	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/optimize-database.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10436	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/my-profile.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10401	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-article.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10402	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-category.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10403	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-comment.php by adding a question mark (?) followed by the payload.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10404	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-field.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10410	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-user.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10405	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-glossary.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10409	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-template.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10408	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/edit-subscriber.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10395	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-group.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10394	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-glossary.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10393	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-field.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10392	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-category.php by adding a question mark (?) followed by the payload.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10454	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/sitemap-generator.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10453	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/search-users.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10452	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/save-article.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10451	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-user.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10450	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-traffic.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10449	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-search.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10414	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/index-attachments.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10448	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-referrers.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10447	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-failed-login.php by adding a question mark (?) followed by the payload.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10413	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/import-html.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10446	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-category.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10445	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-article.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10444	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-article-rated.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10412	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/import-csv.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10443	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-article-printed.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10442	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-article-popular.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10391	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/add-article.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10577	An issue was discovered in Janus through 0.9.1. janus.c has multiple concurrent threads that misuse the source property of a session, leading to a race condition when claiming sessions.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10424	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/manage-fields.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2020-10441	The way URIs are handled in admin/header.php in Chadha PHPKB Standard Multi-Language 9 allows Reflected XSS (injecting arbitrary web script or HTML) in admin/report-article-monthly.php by adding a question mark (?) followed by the payload.	4.8	More Details
CVE-2019-4617	IBM Cloud Automation Manager 3.2.1.0 does not renew a session variable after a successful authentication which could lead to session fixation/hijacking vulnerability. This could force a user to utilize a cookie that may be known to an attacker. IBM X-Force ID: 168645.	4.4	More Details
CVE-2019-14625	Improper access control in on-card storage for the Intel® FPGA Programmable Acceleration Card N3000, all versions, may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2020-0507	Unquoted service path in Intel(R) Graphics Drivers before versions 15.33.49.5100, 15.36.38.5117, 15.40.44.5107, 15.45.30.5103, and 26.20.100.7212 may allow an authenticated user to potentially enable denial of service via local access.	4.4	More Details
CVE-2019-20407	The ConfigureBambooRelease resource in Jira Software and Jira Software Data Center before version 8.6.1 allows authenticated remote attackers to view release version information in projects that they do not have access to through an missing authorisation check.	4.3	More Details
CVE-2019-16107	Missing form token validation in phpBB 3.2.7 allows CSRF in deleting post attachments.	4.3	More Details
CVE-2020-10493	CSRF in admin/edit-glossary.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to edit a glossary term, given the id, via a crafted request.	4.3	More Details
CVE-2020-10484	CSRF in admin/add-field.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to create a custom field via a crafted request.	4.3	More Details
CVE-2020-10486	CSRF in admin/manage-comments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete a comment via a crafted request.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10487	CSRF in admin/manage-glossary.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete a glossary term via a crafted request.	4.3	More Details
CVE-2020-10483	CSRF in admin/ajax-hub.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to post a comment on any article via a crafted request.	4.3	More Details
CVE-2020-10488	CSRF in admin/manage-news.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete a news article via a crafted request.	4.3	More Details
CVE-2020-10489	CSRF in admin/manage-tickets.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete a ticket via a crafted request.	4.3	More Details
CVE-2020-10490	CSRF in admin/manage-departments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete a department via a crafted request.	4.3	More Details
CVE-2020-10491	CSRF in admin/manage-departments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to add a department via a crafted request.	4.3	More Details
CVE-2020-10492	CSRF in admin/manage-templates.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete an article template via a crafted request.	4.3	More Details
CVE-2020-10482	CSRF in admin/add-template.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to add a new article template via a crafted request.	4.3	More Details
CVE-2020-10494	CSRF in admin/edit-news.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to edit a news article, given the id, via a crafted request.	4.3	More Details
CVE-2020-10495	CSRF in admin/edit-template.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to edit an article template, given the id, via a crafted request.	4.3	More Details
CVE-2020-10496	CSRF in admin/edit-article.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to edit an article, given the id, via a crafted request.	4.3	More Details
CVE-2020-10499	CSRF in admin/manage-tickets.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to close any ticket, given the id, via a crafted request.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10500	CSRF in admin/reply-ticket.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to reply to any ticket, given the id, via a crafted request.	4.3	More Details
CVE-2020-10502	CSRF in admin/manage-comments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to approve any comment, given the id, via a crafted request.	4.3	More Details
CVE-2020-10503	CSRF in admin/manage-comments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to disapprove any comment, given the id, via a crafted request.	4.3	More Details
CVE-2020-10504	CSRF in admin/edit-comments.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to edit a comment, given the id, via a crafted request.	4.3	More Details
CVE-2020-10481	CSRF in admin/add-glossary.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to add a new glossary term via a crafted request.	4.3	More Details
CVE-2020-0885	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics Component Information Disclosure Vulnerability'.	4.3	More Details
CVE-2020-10480	CSRF in admin/add-category.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to add a new category via a crafted request.	4.3	More Details
CVE-2019-12278	Opera through 53 on Android allows Address Bar Spoofing. Characters from several languages are displayed in Right-to-Left order, due to mishandling of several Unicode characters. The rendering mechanism, in conjunction with the "first strong character" concept, may improperly operate on a numerical IP address or an alphabetic string, leading to a spoofed URL.	4.3	More Details
CVE-2020-10479	CSRF in admin/add-news.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to add a new news article via a crafted request.	4.3	More Details
CVE-2020-10485	CSRF in admin/manage-articles.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to delete an article via a crafted request.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10575	An issue was discovered in Janus through 0.9.1. plugins/janus_videocall.c in the VideoCall plugin mishandles session management because a race condition causes some references to be freed too early or too many times.	4.2	More Details
CVE-2020-1735	A flaw was found in the Ansible Engine when the fetch module is used. An attacker could intercept the module, inject a new path, and then choose a new destination path on the controller node. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable.	4.2	More Details
CVE-2020-1739	A flaw was found in Ansible 2.7.16 and prior, 2.8.8 and prior, and 2.9.5 and prior when a password is set with the argument "password" of svn module, it is used on svn command line, disclosing to other users within the same node. An attacker could take advantage by reading the cmdline file from that particular PID on the procfs.	3.9	More Details
CVE-2020-1738	A flaw was found in Ansible Engine when the module package or service is used and the parameter 'use' is not specified. If a previous task is executed with a malicious user, the module sent can be selected by the attacker using the ansible facts file. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable.	3.9	More Details
CVE-2020-1740	A flaw was found in Ansible Engine when using Ansible Vault for editing encrypted files. When a user executes "ansible-vault edit", another user on the same computer can read the old and new secret, as it is created in a temporary file with mkstemp and the returned file descriptor is closed and the method write_data is called to write the existing secret in the file. This method will delete the file before recreating it insecurely. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable.	3.9	More Details
CVE-2020-3951	VMware Workstation (15.x before 15.5.2) and Horizon Client for Windows (5.x and prior before 5.4.0) contain a denial-of-service vulnerability due to a heap-overflow issue in Cortado Thinprint. Attackers with non-administrative access to a guest VM with virtual printing enabled may exploit this issue to create a denial-of-service condition of the Thinprint service running on the system where Workstation or Horizon Client is installed.	3.8	More Details
CVE-2020-0884	A spoofing vulnerability exists in Microsoft Visual Studio as it includes a reply URL that is not secured by SSL, aka 'Microsoft Visual Studio Spoofing Vulnerability'.	3.7	More Details
CVE-2019-20494	In cPanel before 82.0.18, Cpanel::Rand::Get can produce a predictable series of numbers (SEC-525).	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6980	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, If Simple Mail Transfer Protocol (SMTP) account data is saved in RSLogix 500, a local attacker with access to a victim's project may be able to gather SMTP server authentication data as it is written to the project file in cleartext.	3.3	More Details
CVE-2020-1720	A flaw was found in PostgreSQL's "ALTER ... DEPENDS ON EXTENSION", where sub-commands did not perform authorization checks. An authenticated attacker could use this flaw in certain configurations to perform drop objects such as function, triggers, et al., leading to database corruption. This issue affects PostgreSQL versions before 12.2, before 11.7, before 10.12 and before 9.6.17.	3.1	More Details
CVE-2020-10459	Path Traversal in admin/assetmanager/assetmanager.php (vulnerable function saved in admin/assetmanager/functions.php) in Chadha PHPKB Standard Multi-Language 9 allows attackers to list the files that are stored on the webserver using a dot-dot-slash sequence (../) via the POST parameter inpCurrFolder.	2.7	More Details
CVE-2020-10457	Path Traversal in admin/imagepaster/image-renaming.php in Chadha PHPKB Standard Multi-Language 9 allows attackers to rename any file on the webserver using a dot-dot-slash sequence (../) via the POST parameter imgName (for the new name) and imgUrl (for the current file to be renamed).	2.7	More Details
CVE-2020-0506	Improper initialization in Intel(R) Graphics Drivers before versions 15.40.44.5107, 15.45.29.5077, and 26.20.100.7000 may allow a privileged user to potentially enable a denial of service via local access.	2.3	More Details
CVE-2020-1736	A flaw was found in Ansible Engine when a file is moved using atomic_move primitive as the file mode cannot be specified. This sets the destination files world-readable if the destination file does not exist and if the file exists, the file could be changed to have less restrictive permissions before the move. This could lead to the disclosure of sensitive data. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable.	2.2	More Details
CVE-2018-19325	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2018-14466. Reason: This candidate is a duplicate of CVE-2018-14466. Notes: All CVE users should reference CVE-2018-14466 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details