SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 24 February 2021

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-27329	Friendica 2021.01 allows SSRF via parse_url?binurl= for DNS lookups or HTTP requests to arbitrary domain names.	10.0	More Details
CVE-2020-2501	A stack-based buffer overflow vulnerability has been reported to affect QNAP NAS devices running Surveillance Station. If exploited, this vulnerability allows attackers to execute arbitrary code. QNAP have already fixed this vulnerability in the following versions: Surveillance Station 5.1.5.4.3 (and later) for ARM CPU NAS (64bit OS) and x86 CPU NAS (64bit OS) Surveillance Station 5.1.5.3.3 (and later) for ARM CPU NAS (32bit OS) and x86 CPU NAS (32bit OS)	9.8	More Details
CVE-2019-25024	OpenRepeater (ORP) before 2.2 allows unauthenticated command injection via shell metacharacters in the functions/ajax_system.php post_service parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27228	An issue was discovered in Shinobi through ocean version 1. lib/auth.js has Incorrect Access Control. Valid API Keys are held in an internal JS Object. Therefore an attacker can use JS Proto Method names (such as constructor or hasOwnProperty) to convince the System that the supplied API Key exists in the underlying JS object, and consequently achieve complete access to User/Admin/Super API functions, as demonstrated by a /super/constructor/accounts/list URI.	9.8	More Details
CVE-2021-3120	An arbitrary file upload vulnerability in the YITH WooCommerce Gift Cards Premium plugin before 3.3.1 for WordPress allows remote attackers to achieve remote code execution on the operating system in the security context of the web server. In order to exploit this vulnerability, an attacker must be able to place a valid Gift Card product into the shopping cart. An uploaded file is placed at a predetermined path on the web server with a user-specified filename and extension. This occurs because the ywgc-upload-picture parameter can have a .php value even though the intention was to only allow uploads of Gift Card images.	9.8	More Details
CVE-2020-21224	A Remote Code Execution vulnerability has been found in Inspur ClusterEngine V4.0. A remote attacker can send a malicious login packet to the control server	9.8	More Details
CVE-2020-11283	A buffer overflow can occur when playing an MKV clip due to lack of input validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.8	More Details
CVE-2020-11272	Before enqueuing a frame to the PE queue for further processing, an entry in a hash table can be deleted and using a stale version later can lead to use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.8	More Details
CVE-2020-11170	Out of bound memory access while playing music playbacks with crafted vorbis content due to improper checks in header extraction in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2020-11163	Possible buffer overflow while updating ikev2 parameters due to lack of check of input validation for certain parameters received from the ePDG server in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26120	Smarty before 3.1.39 allows code injection via an unexpected function name after a {function name= substring.	9.8	More Details
CVE-2021-24115	In Botan before 2.17.3, constant-time computations are not used for certain decoding and encoding operations (base32, base58, base64, and hex).	9.8	More Details
CVE-2021-27514	EyesOfNetwork 5.3-10 uses an integer of between 8 and 10 digits for the session ID, which might be leveraged for brute-force authentication bypass (such as in CVE-2021-27513 exploitation).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20587	Heap-based buffer overflow vulnerability in Mitsubishi Electric FA Engineering Software (CPU Module Logging Configuration Tool versions 1.112R and prior, CW Configurator versions 1.011M and prior, Data Transfer versions 3.44W and prior, EZSocket versions 5.4 and prior, FR Configurator all versions, FR Configurator SW3 all versions, FR Configurator2 versions 1.24A and prior, GT Designer3 Version1(GOT1000) versions 1.250L and prior, GT Designer3 Version1(GOT2000) versions 1.250L and prior, GT SoftGOT1000 Version3 versions 3.245F and prior, GT SoftGOT2000 Version1 versions 1.250L and prior, GX Configurator-DP versions 7.14Q and prior, GX Configurator-QP all versions, GX Developer versions 8.506C and prior, GX Explorer all versions, GX IEC Developer all versions, GX LogViewer versions 1.115U and prior, GX RemoteService-I all versions, GX Works2 versions 1.597X and prior, GX Works3 versions 1.070Y and prior, iQ Monozukuri ANDON (Data Transfer) all versions, iQ Monozukuri Process Remote Monitoring (Data Transfer) all versions, M_CommDTM-HART all versions, M_CommDTM-IO-Link versions 1.03D and prior, MELFA-Works versions 4.4 and prior, MELSEC WinCPU Setting Utility all versions, MELSOFT EM Software Development Kit (EM Configurator) versions 1.015R and prior, MELSOFT Navigator versions 2.74C and prior, MH11 SettingTool Version2 versions 2.004E and prior, MI Configurator versions 1.004E and prior, MT Works2 versions 1.167Z and prior, MX Component versions 5.001B and prior, Network Interface Board CC IE Control utility versions 1.29F and prior, Network Interface Board CC IE Field Utility versions 1.16S and prior, Network Interface Board CC-Link Ver.2 Utility versions 1.23Z and prior, Network Interface Board MNETH utility versions 34L and prior, PX Developer versions 1.53F and prior, RT ToolBox2 versions 3.73B and prior, RT ToolBox3 versions 1.82L and prior, Setting/monitoring tools for the C Controller module (SW4PVC-CCPU) versions 4.12N and prior and SLMP Data Collector versions 1.04E and prior) allows a remote unauthenticated attacker to cause a DoS condition of the software products, and possibly to execute a malicious program on the personal computer running the software products although it has not been reproduced, by spoofing MELSEC, GOT or FREQROL and returning crafted reply packets.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20588	Improper handling of length parameter inconsistency vulnerability in Mitsubishi Electric FA Engineering Software(CPU Module Logging Configuration Tool versions 1.112R and prior, CW Configurator versions 1.011M and prior, Data Transfer versions 3.44W and prior, EZSocket versions 5.4 and prior, FR Configurator all versions, FR Configurator SW3 all versions, FR Configurator2 versions 1.24A and prior, GT Designer3 Version1(GOT1000) versions 1.250L and prior, GT Designer3 Version1(GOT2000) versions 1.250L and prior, GT SoftGOT1000 Version3 versions 3.245F and prior, GT SoftGOT2000 Version1 versions 1.250L and prior, GX Configurator-DP versions 7.14Q and prior, GX Configurator-QP all versions, GX Developer versions 8.506C and prior, GX Explorer all versions, GX IEC Developer all versions, GX LogViewer versions 1.115U and prior, GX RemoteService-I all versions, GX Works2 versions 1.597X and prior, GX Works3 versions 1.070Y and prior, iQ Monozukuri ANDON (Data Transfer) all versions, iQ Monozukuri Process Remote Monitoring (Data Transfer) all versions, M_CommDTM-HART all versions, M_CommDTM-IO-Link versions 1.03D and prior, MELFA-Works versions 4.4 and prior, MELSEC WinCPU Setting Utility all versions, MELSOFT EM Software Development Kit (EM Configurator) versions 1.015R and prior, MELSOFT Navigator versions 2.74C and prior, MH11 SettingTool Version2 versions 2.004E and prior, MI Configurator versions 1.004E and prior, MT Works2 versions 1.167Z and prior, MX Component versions 5.001B and prior, Network Interface Board CC IE Control utility versions 1.29F and prior, Network Interface Board CC IE Field Utility versions 1.16S and prior, Network Interface Board CC-Link Ver.2 Utility versions 1.23Z and prior, Network Interface Board MNETH utility versions 34L and prior, PX Developer versions 1.53F and prior, RT ToolBox2 versions 3.73B and prior, RT ToolBox3 versions 1.82L and prior, Setting/monitoring tools for the C Controller module (SW4PVC-CCPU) versions 4.12N and prior and SLMP Data Collector versions 1.04E and prior) allows a remote unauthenticated attacker to cause a DoS condition of the software products, and possibly to execute a malicious program on the personal computer running the software products although it has not been reproduced, by spoofing MELSEC, GOT or FREQROL and returning crafted reply packets.	9.8	More Details
CVE-2021-26747	Netis WF2780 2.3.40404 and WF2411 1.1.29629 devices allow Shell Metacharacter Injection into the ping command, leading to remote code execution.	9.8	More Details
CVE-2021-27335	KollectApps before 4.8.16c is affected by insecure Java deserialization, leading to Remote Code Execution via a ysoserial.payloads.CommonsCollections parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27378	An issue was discovered in the rand_core crate before 0.6.2 for Rust. Because read_u32_into and read_u64_into mishandle certain buffer-length checks, a random number generator may be seeded with too little data.	9.8	More Details
CVE-2021-27377	An issue was discovered in the yottadb crate before 1.2.0 for Rust. For some memory-allocation patterns, ydb_subscript_next_st and ydb_subscript_prev_st have a use-after-free.	9.8	More Details
CVE-2021-27376	An issue was discovered in the nb-connect crate before 1.0.3 for Rust. It may have invalid memory access for certain versions of the standard library because it relies on a direct cast of std::net::SocketAddrV4 and std::net::SocketAddrV6 data structures.	9.8	More Details
CVE-2021-27362	The WPG plugin before 3.1.0.0 for IrfanView 4.57 has a Read Access Violation on Control Flow starting at WPG!ReadWPG_W+0x0000000000000133, which might allow remote attackers to execute arbitrary code.	9.8	More Details
CVE-2021-26809	PHPGurukul Car Rental Project version 2.0 suffers from a remote shell upload vulnerability in changeimage1.php.	9.8	More Details
CVE-2021-25779	Baby Care System v1.0 is vulnerable to SQL injection via the 'id' parameter on the contentsectionpage.php page.	9.8	More Details
CVE-2020-35339	In 74cms version 5.0.1, there is a remote code execution vulnerability in /Application/Admin/Controller/ConfigController.class.php and /ThinkPHP/Common/functions.php where attackers can obtain server permissions and control the server.	9.8	More Details
CVE-2021-22855	The specific function of HR Portal of Soar Cloud System accepts any type of object to be deserialized. Attackers can send malicious serialized objects to execute arbitrary commands.	9.8	More Details
CVE-2021-22856	The CGE property management system contains SQL Injection vulnerabilities. Remote attackers can inject SQL commands into the parameters in Cookie and obtain data in the database without privilege.	9.8	More Details
CVE-2021-21150	Use after free in Downloads in Google Chrome on Windows prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21155	Heap buffer overflow in Tab Strip in Google Chrome on Windows prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-21154	Heap buffer overflow in Tab Strip in Google Chrome prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-3210	components/Modals/HelpTexts/GenericAll/GenericAll.jsx in Bloodhound <= 4.0.1 allows remote attackers to execute arbitrary system commands when the victim imports a malicious data file containing JavaScript in the objectId parameter.	9.6	More Details
CVE-2021-21151	Use after free in Payments in Google Chrome prior to 88.0.4324.182 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-11275	Possible buffer over-read while parsing quiet IE in Rx beacon frame due to improper check of IE length in received beacon in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	9.1	More Details
CVE-2020-11276	Possible buffer over read while processing P2P IE and NOA attribute of beacon and probe response frames due to improper validation of P2P IE and NOA attribute lengths in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	9.1	More Details
CVE-2020-28490	The package async-git before 1.13.2 are vulnerable to Command Injection via shell meta-characters (back-ticks). For example: git.reset('atouch HACKEDb')	9.1	More Details
CVE-2021-27582	org/mitre/oauth2/web/OAuthConfirmationController.java in the OpenID Connect server implementation for MITREid Connect through 1.3.3 contains a Mass Assignment (aka Autobinding) vulnerability. This arises due to unsafe usage of the @ModelAttribute annotation during the OAuth authorization flow, in which HTTP request parameters affect an authorizationRequest.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23885	Privilege escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.8 allows an authenticated user to gain elevated privileges through the User Interface and execute commands on the appliance via incorrect improper neutralization of user input in the troubleshooting page.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-13551	An exploitable local privilege elevation vulnerability exists in the file system permissions of Advantech WebAccess/SCADA 9.0.1 installation. In privilege escalation via PostgreSQL executable, an attacker can either replace binary or loaded modules to execute code with NT SYSTEM privilege.	8.8	More Details
CVE-2020-12339	Insufficient control flow management in the API for the Intel(R) Collaboration Suite for WebRTC before version 4.3.1 may allow an authenticated user to potentially enable escalation of privilege via network access.	8.8	More Details
CVE-2021-21157	Use after free in Web Sockets in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21153	Stack buffer overflow in GPU Process in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	8.8	More Details
CVE-2021-21152	Heap buffer overflow in Media in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21149	Stack buffer overflow in Data Transfer in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.	8.8	More Details
CVE-2021-26068	An endpoint in Atlassian Jira Server for Slack plugin from version 0.0.3 before version 2.0.15 allows remote attackers to execute arbitrary code via a template injection vulnerability.	8.8	More Details
CVE-2020-9306	Tesla SolarCity Solar Monitoring Gateway through 5.46.43 has a "Use of Hard-coded Credentials" issue because Digi ConnectPort X2e uses a .pyc file to store the cleartext password for the python user account.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20443	IBM Maximo for Civil Infrastructure 7.6.2 includes executable functionality (such as a library) from a source that is outside of the intended control sphere. IBM X-Force ID: 196619.	8.8	More Details
CVE-2020-11269	Possible memory corruption while processing EAPOL frames due to lack of validation of key length before using it in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	8.8	More Details
CVE-2020-36247	Open OnDemand before 1.5.7 and 1.6.x before 1.6.22 allows CSRF.	8.8	More Details
CVE-2020-11177	User can overwrite Security Code NV item without knowing current SPC due to improper validation of SPC code setting and device lock in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.8	More Details
CVE-2021-27513	The module admin_ITSM in EyesOfNetwork 5.3-10 allows remote authenticated users to upload arbitrary .xml.php files because it relies on "le filtre userside."	8.8	More Details
CVE-2020-28248	An integer overflow in the PngImg::InitStorage_() function of png-img before 3.1.0 leads to an under-allocation of heap memory and subsequently an exploitable heap-based buffer overflow when loading a crafted PNG file.	8.8	More Details
CVE-2020-27997	An issue was discovered in SmartStoreNET before 4.1.0. Lack of Cross Site Request Forgery (CSRF) protection may lead to elevation of privileges (e.g., /admin/customer/create to create an admin account).	8.8	More Details
CVE-2020-24617	Mailtrain through 1.24.1 allows SQL Injection in statsClickedSubscribersByColumn in lib/models/campaigns.js via /campaigns/clicked/ajax because variable column names are not properly escaped.	8.8	More Details
CVE-2020-12873	An issue was discovered in Alfresco Enterprise Content Management (ECM) before 6.2.1. A user with privileges to edit a FreeMarker template (e.g., a webscript) may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running Alfresco.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25690	An out-of-bounds write flaw was found in FontForge in versions before 20200314 while parsing SFD files containing certain LayerCount tokens. This flaw allows an attacker to manipulate the memory allocated on the heap, causing the application to crash or execute arbitrary code. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	8.8	More Details
CVE-2021-21156	Heap buffer overflow in V8 in Google Chrome prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted script.	8.8	More Details
CVE-2020-13555	An exploitable local privilege elevation vulnerability exists in the file system permissions of Advantech WebAccess/SCADA 9.0.1 installation. In COM Server Application Privilege Escalation, an attacker can either replace binary or loaded modules to execute code with NT SYSTEM privilege.	8.8	More Details
CVE-2021-26594	In Directus 8.x through 8.8.1, an attacker can switch to the administrator role (via the PATCH method) without any control by the back end. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	8.8	More Details
CVE-2020-13552	An exploitable local privilege elevation vulnerability exists in the file system permissions of Advantech WebAccess/SCADA 9.0.1 installation. In privilege escalation via multiple service executables in installation folder of WebAccess, an attacker can either replace binary or loaded modules to execute code with NT SYSTEM privilege.	8.8	More Details
CVE-2020-36245	GramAddict through 1.2.3 allows remote attackers to execute arbitrary code because of use of UIAutomator2 and ATX-Agent. The attacker must be able to reach TCP port 7912, e.g., by being on the same Wi-Fi network.	8.8	More Details
CVE-2020-25161	The WADashboard component of WebAccess/SCADA Versions 9.0 and prior may allow an attacker to control or influence a path used in an operation on the filesystem and remotely execute code as an administrator.	8.8	More Details
CVE-2021-3396	OpenNMS Meridian 2016, 2017, 2018 before 2018.1.25, 2019 before 2019.1.16, and 2020 before 2020.1.5, Horizon 1.2 through 27.0.4, and Newts <1.5.3 has Incorrect Access Control, which allows local and remote code execution using JEXL expressions.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20182	A privilege escalation flaw was found in openshift4/ose-docker-builder. The build container runs with high privileges using a chrooted environment instead of runc. If an attacker can gain access to this build container, they can potentially utilize the raw devices of the underlying node, such as the network and storage devices, to at least escalate their privileges to that of the cluster admin. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	8.8	More Details
CVE-2021-22858	Attackers can access the CGE account management function without privilege for permission elevation and execute arbitrary commands or files after obtaining user permissions.	8.8	More Details
CVE-2021-22112	Spring Security 5.4.x prior to 5.4.4, 5.3.x prior to 5.3.8.RELEASE, 5.2.x prior to 5.2.9.RELEASE, and older unsupported versions can fail to save the SecurityContext if it is changed more than once in a single request.A malicious user cannot cause the bug to happen (it must be programmed in). However, if the application's intent is to only allow the user to run with elevated privileges in a small portion of the application, the bug can be leveraged to extend those privileges to the rest of the application.	8.8	More Details
CVE-2020-13553	An exploitable local privilege elevation vulnerability exists in the file system permissions of Advantech WebAccess/SCADA 9.0.1 installation. In webvrpcs Run Key Privilege Escalation in installation folder of WebAccess, an attacker can either replace binary or loaded modules to execute code with NT SYSTEM privilege.	8.8	More Details
CVE-2021-23342	This affects the package docsify before 4.12.0. It is possible to bypass the remediation done by CVE-2020-7680 and execute malicious JavaScript through the following methods 1) When parsing HTML from remote URLs, the HTML code on the main page is sanitized, but this sanitization is not taking place in the sidebar. 2) The isURL external check can be bypassed by inserting more “////” characters	8.6	More Details
CVE-2020-10252	An issue was discovered in ownCloud before 10.4. Because of an SSRF issue (via the apps/files_sharing/external remote parameter), an authenticated attacker can interact with local services blindly (aka Blind SSRF) or conduct a Denial Of Service attack.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8625	BIND servers are vulnerable if they are running an affected version and are configured to use GSS-TSIG features. In a configuration which uses BIND's default settings the vulnerable code path is not exposed, but a server can be rendered vulnerable by explicitly setting valid values for the tkey-gssapi-keytab or tkey-gssapi-credentialconfiguration options. Although the default configuration is not vulnerable, GSS-TSIG is frequently used in networks where BIND is integrated with Samba, as well as in mixed-server environments that combine BIND servers with Active Directory domain controllers. The most likely outcome of a successful exploitation of the vulnerability is a crash of the named process. However, remote code execution, while unproven, is theoretically possible. Affects: BIND 9.5.0 -> 9.11.27, 9.12.0 -> 9.16.11, and versions BIND 9.11.3-S1 -> 9.11.27-S1 and 9.16.8-S1 -> 9.16.11-S1 of BIND Supported Preview Edition. Also release versions 9.17.0 -> 9.17.1 of the BIND 9.17 development branch	8.1	More Details
CVE-2021-20198	A flaw was found in the OpenShift Installer before version v0.9.0-master.0.20210125200451-95101da940b0. During installation of OpenShift Container Platform 4 clusters, bootstrap nodes are provisioned with anonymous authentication enabled on kubelet port 10250. A remote attacker able to reach this port during installation can make unauthenticated `/exec` requests to execute arbitrary commands within running containers. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	8.1	More Details
CVE-2020-7848	The EFM ipTIME C200 IP Camera is affected by a Command Injection vulnerability in /login.cgi?logout=1 script. To exploit this vulnerability, an attacker can send a GET request that executes arbitrary OS commands via cookie value.	8.0	More Details
CVE-2020-7849	A vulnerability of uPrism.io CURIX(Video conferecing solution) could allow an unauthenticated attacker to execute arbitrary code. This vulnerability is due to insufficient input(server domain) validation. An attacker could exploit this vulnerability through crafted URL.	8.0	More Details
CVE-2021-21512	Dell EMC PowerProtect Cyber Recovery, version 19.7.0.1, contains an Information Disclosure vulnerability. A locally authenticated high privileged Cyber Recovery user may potentially exploit this vulnerability leading to the takeover of the notification email account.	7.9	More Details
CVE-2021-27138	The boot loader in Das U-Boot before 2021.04-rc2 mishandles use of unit addresses in a FIT.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24908	Checkmk before 1.6.0p17 allows local users to obtain SYSTEM privileges via a Trojan horse shell script in the %PROGRAMDATA%\checkmk\agent\local directory.	7.8	More Details
CVE-2020-36246	Amaze File Manager before 3.5.1 allows attackers to obtain root privileges via shell metacharacters in a symbolic link.	7.8	More Details
CVE-2020-19513	Buffer overflow in FinalWire Ltd AIDA64 Engineer 6.00.5100 allows attackers to execute arbitrary code by creating a crafted input that will overwrite the SEH handler.	7.8	More Details
CVE-2020-12878	Digi ConnectPort X2e before 3.2.30.6 allows an attacker to escalate privileges from the python user to root via a symlink attack that uses chown, related to /etc/init.d/S50dropbear.sh and the /WEB/python/.ssh directory.	7.8	More Details
CVE-2021-27379	An issue was discovered in Xen through 4.11.x, allowing x86 Intel HVM guest OS users to achieve unintended read/write DMA access, and possibly cause a denial of service (host OS crash) or gain privileges. This occurs because a backport missed a flush, and thus IOMMU updates were not always correct. NOTE: this issue exists because of an incomplete fix for CVE-2020-15565.	7.8	More Details
CVE-2020-29664	A command injection issue in dji_sys in DJI Mavic 2 Remote Controller before firmware version 01.00.0510 allows for code execution via a malicious firmware upgrade packet.	7.8	More Details
CVE-2021-26720	avahi-daemon-check-dns.sh in the Debian avahi package through 0.8-4 is executed as root via /etc/network/if-up.d/avahi-daemon, and allows a local attacker to cause a denial of service or create arbitrary empty files via a symlink attack on files under /run/avahi-daemon. NOTE: this only affects the packaging for Debian GNU/Linux (used indirectly by SUSE), not the upstream Avahi product.	7.8	More Details
CVE-2020-13549	An exploitable local privilege elevation vulnerability exists in the file system permissions of Sytech XL Reporter v14.0.1 install directory. Depending on the vector chosen, an attacker can overwrite service executables and execute arbitrary code with privileges of user set to run the service or replace other files within the installation folder, which would allow for local privilege escalation.	7.8	More Details
CVE-2021-27097	The boot loader in Das U-Boot before 2021.04-rc2 mishandles a modified FIT.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36233	The Microsoft Windows Installer for Atlassian Bitbucket Server and Data Center before version 6.10.9, 7.x before 7.6.4, and from version 7.7.0 before 7.10.1 allows local attackers to escalate privileges because of weak permissions on the installation directory.	7.8	More Details
CVE-2021-26930	An issue was discovered in the Linux kernel 3.11 through 5.10.16, as used by Xen. To service requests to the PV backend, the driver maps grant references provided by the frontend. In this process, errors may be encountered. In one case, an error encountered earlier might be discarded by later processing, resulting in the caller assuming successful mapping, and hence subsequent operations trying to access space that wasn't mapped. In another case, internal state would be insufficiently updated, preventing safe recovery from the error. This affects drivers/block/xen-blkback/blkback.c.	7.8	More Details
CVE-2020-25171	The affected Fuji Electric V-Server Lite versions prior to 3.3.24.0 are vulnerable to an out-of-bounds write, which may allow an attacker to remotely execute arbitrary code.	7.8	More Details
CVE-2021-22647	Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to multiple out-of-bounds write issues while processing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-20194	There is a vulnerability in the linux kernel versions higher than 5.2 (if kernel compiled with config params CONFIG_BPF_SYSCALL=y , CONFIG_BPF=y , CONFIG_CGROUPS=y , CONFIG_CGROUP_BPF=y , CONFIG_HARDENED_USERCOPY not set, and BPF hook to getsockopt is registered). As result of BPF execution, the local user can trigger bug in __cgroup_bpf_run_filter_getsockopt() function that can lead to heap overflow (because of non-hardened usercopy). The impact of attack could be deny of service or possibly privileges escalation.	7.8	More Details
CVE-2021-26677	A local authenticated escalation of privilege vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in ClearPass OnGuard could allow local authenticated users on a Windows platform to elevate their privileges. A successful exploit could allow an attacker to execute arbitrary code with SYSTEM level privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28587	A specially crafted document can cause the document parser to copy data from a particular record type into a static-sized buffer within an object that is smaller than the size used for the copy, which will cause a heap-based buffer overflow. An attacker can entice the victim to open a document to trigger this vulnerability. This affects SoftMaker Software GmbH SoftMaker Office PlanMaker 2021 (Revision 1014).	7.8	More Details
CVE-2021-27579	Snow Inventory Agent through 6.7.0 on Windows uses CPUID to report on processor types and versions that may be deployed and in use across an IT environment. A privilege-escalation vulnerability exists if CPUID is enabled, and thus it should be disabled via configuration settings.	7.8	More Details
CVE-2021-22651	When loading a specially crafted file, Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are, while processing the extraction of temporary files, suffering from a directory traversal vulnerability, which allows an attacker to store arbitrary scripts into automatic startup folders.	7.8	More Details
CVE-2021-20226	A use-after-free flaw was found in the io_uring in Linux kernel, where a local attacker with a user privilege could cause a denial of service problem on the system The issue results from the lack of validating the existence of an object prior to performing operations on the object by not incrementing the file reference counter while in use. The highest threat from this vulnerability is to data integrity, confidentiality and system availability.	7.8	More Details
CVE-2020-16243	Multiple buffer overflow vulnerabilities exist when LeviStudioU (Version 2019-09-21 and prior) processes project files. Opening a specially crafted project file could allow an attacker to exploit and execute code under the privileges of the application.	7.8	More Details
CVE-2021-25630	"loolforkit" is a privileged program that is supposed to be run by a special, non-privileged "lool" user. Before doing anything else "loolforkit" checks, if it was invoked by the "lool" user, and refuses to run with privileges, if it's not the case. In the vulnerable version of "loolforkit" this check was wrong, so a normal user could start "loolforkit" and eventually get local root privileges.	7.8	More Details
CVE-2021-22649	Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 have multiple NULL pointer dereference issues while processing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22645	Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to an attack because the .bip documents display a “load” command, which can be pointed to a .dll from a remote network share. As a result, the .dll entry point can be executed without sufficient UI warning.	7.8	More Details
CVE-2020-11187	Possible memory corruption in BSI module due to improper validation of parameter count in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile	7.8	More Details
CVE-2021-22643	Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2020-24175	Buffer overflow in Yz1 0.30 and 0.32, as used in IZArc 4.4, ZipGenius 6.3.2.3116, and Explzh (extension) 8.14, allows attackers to execute arbitrary code via a crafted archive file, related to filename handling.	7.8	More Details
CVE-2020-11282	Improper access control when using mmap with the kgsl driver with a special offset value that can be provided to map the memstore of the GPU to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details
CVE-2020-11271	Possible out of bounds while accessing global control elements due to race condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.8	More Details
CVE-2020-11253	Arbitrary memory write issue in video driver while setting the internal buffers in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	7.8	More Details
CVE-2020-11223	Out of bound in camera driver due to lack of check of validation of array index before copying into array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11204	Possible memory corruption and information leakage in sub-system due to lack of check for validity and boundary compliance for parameters that are read from shared MSG RAM in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.8	More Details
CVE-2021-1366	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack on an affected device if the VPN Posture (HostScan) Module is installed on the AnyConnect client. This vulnerability is due to insufficient validation of resources that are loaded by the application at run time. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected machine with SYSTEM privileges. To exploit this vulnerability, the attacker needs valid credentials on the Windows system.	7.8	More Details
CVE-2020-11194	Possible out of bound access in TA while processing a command from NS side due to improper length check of response buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.8	More Details
CVE-2020-11195	Out of bound write and read in TA while processing command from NS side due to improper length check on command and response buffers in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	7.8	More Details
CVE-2021-3410	A flaw was found in libcaca v0.99.beta19. A buffer overflow issue in caca_resize function in libcaca/caca/canvas.c may lead to local execution of arbitrary code in the user context.	7.8	More Details
CVE-2020-12366	Insufficient input validation in some Intel(R) Graphics Drivers before version 27.20.100.8587 may allow a privileged user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2020-24462	Out of bounds write in the Intel(R) Graphics Driver before version 15.33.53.5161, 15.36.40.5162, 15.40.47.5166, 15.45.33.5164 and 27.20.100.8336 may allow an authenticated user to potentially enable an escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12377	Insufficient input validation in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.47 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-0521	Insufficient control flow management in some Intel(R) Graphics Drivers before version 15.45.32.5145 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-12380	Out of bounds read in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.47 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-0109	Insecure inherited permissions for the Intel(R) SOC driver package for STK1A32SC before version 604 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-12384	Improper access control in some Intel(R) Graphics Drivers before version 26.20.100.8476 may allow an authenticated user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2020-24485	Improper conditions check in the Intel(R) FPGA OPAE Driver for Linux before kernel version 4.17 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-24481	Insecure inherited permissions for the Intel(R) Quartus Prime Pro and Standard edition software may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-8678	Improper access control for Intel(R) Graphics Drivers before version 15.45.33.5164 and 27.20.100.8280 may allow an authenticated user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2020-12385	Improper input validation in some Intel(R) Graphics Drivers before version 26.20.100.8141 may allow a privileged user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-26934	An issue was discovered in the Linux kernel 4.18 through 5.10.16, as used by Xen. The backend allocation (aka be-alloc) mode of the drm_xen_front drivers was not meant to be a supported configuration, but this wasn't stated accordingly in its support status entry.	7.8	More Details
CVE-2020-12369	Out of bound write in some Intel(R) Graphics Drivers before version 26.20.100.8336 may allow a privileged user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12368	Integer overflow in some Intel(R) Graphics Drivers before version 26.20.100.8141 may allow a privileged user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2020-12367	Integer overflow in some Intel(R) Graphics Drivers before version 26.20.100.8476 may allow a privileged user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2020-0544	Insufficient control flow management in the kernel mode driver for some Intel(R) Graphics Drivers before version 15.36.39.5145 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-24450	Improper conditions check in some Intel(R) Graphics Drivers before versions 26.20.100.8141, 15.45.32.5145 and 15.40.46.5144 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-24453	Improper input validation in the Intel(R) EPID SDK before version 8, may allow an authenticated user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2020-12362	Integer overflow in the firmware for some Intel(R) Graphics Drivers for Windows * before version 26.20.100.7212 and before Linux kernel version 5.5 may allow a privileged user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2020-13550	A local file inclusion vulnerability exists in the installation functionality of Advantech WebAccess/SCADA 9.0.1. A specially crafted application can lead to information disclosure. An attacker can send an authenticated HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2020-11287	Allowing RTT frames to be linked with non randomized MAC address by comparing the sequence numbers can lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-26712	Incorrect access controls in res_srtp.c in Sangoma Asterisk 13.38.1, 16.16.0, 17.9.1, and 18.2.0 and Certified Asterisk 16.8-cert5 allow a remote unauthenticated attacker to prematurely terminate secure calls by replaying SRTP packets.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11296	Arithmetic overflow can happen while processing NOA IE due to improper error handling in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-26717	An issue was discovered in Sangoma Asterisk 16.x before 16.16.1, 17.x before 17.9.2, and 18.x before 18.2.1 and Certified Asterisk before 16.8-cert6. When re-negotiating for T.38, if the initial remote response was delayed just enough, Asterisk would send both audio and T.38 in the SDP. If this happened, and the remote responded with a declined T.38 stream, then Asterisk would crash.	7.5	More Details
CVE-2020-11280	Denial of service while processing fine timing measurement request (FTMR) frame with reserved bits set in the FTM parameter IE due to improper error handling in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2020-11297	Denial of service in WLAN module due to improper check of subtypes in logic where excessive frames are dropped in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	7.5	More Details
CVE-2020-28491	This affects the package com.fasterxml.jackson.dataformat:jackson-dataformat-cbor from 0 and before 2.11.4, from 2.12.0-rc1 and before 2.12.1. Unchecked allocation of byte buffer can cause a java.lang.OutOfMemoryError exception.	7.5	More Details
CVE-2020-11281	Allowing RTT frames to be linked with non randomized MAC address by comparing the sequence numbers can lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-23341	The package prismjs before 1.23.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the prism-asciidoc, prism-rest, prism-tap and prism-eiffel components.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11278	Possible denial of service while handling host WMI command due to improper validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-27405	A ReDoS (regular expression denial of service) flaw was found in the @progfay/scrapbox-parser package before 6.0.3 for Node.js.	7.5	More Details
CVE-2020-11270	Possible denial of service due to RTT responder consistently rejects all FTMR by transmitting FTM1 with failure status in the FTM parameter IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2020-24482	Improper buffer restrictions in firmware for Intel(R) 7360 Cell Modem before UDE version 9.4.370 may allow unauthenticated user to potentially enable denial of service via network access.	7.5	More Details
CVE-2021-26296	In the default configuration, Apache MyFaces Core versions 2.2.0 to 2.2.13, 2.3.0 to 2.3.7, 2.3-next-M1 to 2.3-next-M4, and 3.0.0-RC1 use cryptographically weak implicit and explicit cross-site request forgery (CSRF) tokens. Due to that limitation, it is possible (although difficult) for an attacker to calculate a future CSRF token value and to use that value to trick a user into executing unwanted actions on an application.	7.5	More Details
CVE-2021-22702	A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.	7.5	More Details
CVE-2021-22703	A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36002	Seat-Reservation-System 1.0 has a SQL injection vulnerability in index.php in the id parameter where attackers can obtain sensitive database information.	7.5	More Details
CVE-2020-9050	Path Traversal vulnerability exists in Metasys Reporting Engine (MRE) Web Services which could allow a remote unauthenticated attacker to access and download arbitrary files from the system.	7.5	More Details
CVE-2020-35556	An issue was discovered in Acronis Cyber Protect before 15 Update 1 build 26172. Because the local notification service misconfigures CORS, information disclosure can occur.	7.5	More Details
CVE-2021-26119	Smarty before 3.1.39 allows a Sandbox Escape because $smarty.template_object can be accessed in sandbox mode.	7.5	More Details
CVE-2021-27516	URI.js (aka urijs) before 1.19.6 mishandles certain uses of backslash such as http:\/ and interprets the URI as a relative path.	7.5	More Details
CVE-2020-36249	The File Firewall before 2.8.0 for ownCloud Server does not properly enforce file-type restrictions for public shares.	7.5	More Details
CVE-2021-27509	In Visualware MyConnection Server before 11.0b build 5382, each published report is not associated with its own access code.	7.5	More Details
CVE-2021-22882	UniFi Protect before v1.17.1 allows an attacker to use spoofed cameras to perform a denial-of-service attack that may cause the UniFi Protect controller to crash.	7.5	More Details
CVE-2020-27782	A flaw was found in the Undertow AJP connector. Malicious requests and abrupt connection closes could be triggered by an attacker using query strings with non-RFC compliant characters resulting in a denial of service. The highest threat from this vulnerability is to system availability. This affects Undertow 2.1.5.SP1, 2.0.33.SP2, and 2.2.3.SP1.	7.5	More Details
CVE-2021-27374	VertiGIS WebOffice 10.7 SP1 before patch20210202 and 10.8 SP1 before patch20210207 allows attackers to achieve "Zugriff auf Inhalte der WebOffice Applikation."	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26593	In Directus 8.x through 8.8.1, an attacker can see all users in the CMS using the API /users/{id}. For each call, they get in response a lot of information about the user (such as email address, first name, and last name) but also the secret for 2FA if one exists. This secret can be regenerated. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	7.5	More Details
CVE-2021-22857	The CGE page with download function contains a Directory Traversal vulnerability. Attackers can use this loophole to download system files arbitrarily.	7.5	More Details
CVE-2021-27224	The WPG plugin before 3.1.0.0 for IrfanView 4.57 has a user-mode write access violation starting at WPG+0x0000000000012ec6, which might allow remote attackers to execute arbitrary code.	7.5	More Details
CVE-2021-22854	The HR Portal of Soar Cloud System fails to filter specific parameters. Remote attackers can inject SQL syntax and obtain all data in the database without privilege.	7.5	More Details
CVE-2021-20230	A flaw was found in stunnel before 5.57, where it improperly validates client certificates when it is configured to use both redirect and verifyChain options. This flaw allows an attacker with a certificate signed by a Certificate Authority, which is not the one accepted by the stunnel server, to access the tunneled service instead of being redirected to the address specified in the redirect option. The highest threat from this vulnerability is to confidentiality.	7.5	More Details
CVE-2021-27367	Controller/Backend/FileEditController.php and Controller/Backend/FilemanagerController.php in Bolt before 4.1.13 allow Directory Traversal.	7.5	More Details
CVE-2020-36003	The id parameter in detail.php of Online Book Store v1.0 is vulnerable to union-based blind SQL injection, which leads to the ability to retrieve all databases.	7.5	More Details
CVE-2021-3252	KACO New Energy XP100U Up to XP-JAVA 2.0 is affected by incorrect access control. Credentials will always be returned in plain-text from the local server during the KACO XP100U authentication process, regardless of whatever passwords have been provided, which leads to an information disclosure vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28496	This affects the package three before 0.125.0. This can happen when handling rgb or hsl colors. PoC: var three = require('three') function build_blank (n) { var ret = "rgb(" for (var i = 0; i < n; i++) { ret += " " } return ret + ""; } var Color = three.Color var time = Date.now(); new Color(build_blank(50000)) var time_cost = Date.now() - time; console.log(time_cost+" ms")	7.5	More Details
CVE-2021-20354	IBM WebSphere Application Server 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 194883.	7.5	More Details
CVE-2021-20247	A flaw was found in mbsync before v1.3.5 and v1.4.1. Validations of the mailbox names returned by IMAP LIST/LSUB do not occur allowing a malicious or compromised server to use specially crafted mailbox names containing '..' path components to access data outside the designated mailbox on the opposite end of the synchronization channel. The highest threat from this vulnerability is to data confidentiality and integrity.	7.4	More Details
CVE-2020-7847	The ipTIME NAS product allows an arbitrary file upload vulnerability in the Manage Bulletins/Upload feature, which can be leveraged to gain remote code execution. This issue affects: pTIME NAS 1.4.36.	7.4	More Details
CVE-2020-35681	Django Channels 3.x before 3.0.3 allows remote attackers to obtain sensitive information from a different request scope. The legacy channels.http.AsgiHandler class, used for handling HTTP type requests in an ASGI environment prior to Django 3.0, did not correctly separate request scopes in Channels 3.0. In many cases this would result in a crash but, with correct timing, responses could be sent to the wrong client, resulting in potential leakage of session identifiers and other sensitive data. Note that this affects only the legacy Channels provided class, and not Django's similar ASGIHandler, available from Django 3.0.	7.4	More Details
CVE-2020-11277	Possible race condition during async fastrpc session after sending RPC message due to the fastrpc ctx gets free during async session in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile	7.4	More Details
CVE-2021-26911	core/imap/MCIMAPSession.cpp in Canary Mail before 3.22 has Missing SSL Certificate Validation for IMAP in STARTTLS mode.	7.4	More Details
CVE-2020-28429	All versions of package geojson2kml are vulnerable to Command Injection via the index.js file. PoC: var a =require("geojson2kml"); a("./","& touch JHU",function(){})	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24451	Uncontrolled search path in the Intel(R) Optane(TM) DC Persistent Memory installer for Windows* before version 1.00.00.3506 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.3	More Details
CVE-2020-28499	All versions of package merge are vulnerable to Prototype Pollution via _recursiveMerge .	7.3	More Details
CVE-2020-14359	A vulnerability was found in all versions of Keycloak Gatekeeper, where on using lower case HTTP headers (via cURL) an attacker can bypass our Gatekeeper. Lower case headers are also accepted by some webservers (e.g. Jetty). This means there is no protection when we put a Gatekeeper in front of a Jetty server and use lowercase headers.	7.3	More Details
CVE-2021-20655	FileZen (V3.0.0 to V4.2.7 and V5.0.0 to V5.0.2) allows a remote attacker with administrator rights to execute arbitrary OS commands via unspecified vectors.	7.2	More Details
CVE-2021-26679	A remote authenticated command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the ClearPass web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	More Details
CVE-2021-26680	A remote authenticated command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the ClearPass web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	More Details
CVE-2021-26683	A remote authenticated command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the ClearPass web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3149	On Netshield NANO 25 10.2.18 devices, /usr/local/webmin/System/manual_ping.cgi allows OS command injection (after authentication by the attacker) because the system C library function is used unsafely.	7.2	More Details
CVE-2021-26684	A remote authenticated command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the ClearPass web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	More Details
CVE-2021-26681	A remote authenticated command Injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the ClearPass CLI could allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	More Details
CVE-2021-25780	An arbitrary file upload vulnerability has been identified in posts.php in Baby Care System 1.0. The vulnerability could be exploited by an remote attacker to upload content to the server, including PHP files, which could result in command execution and obtaining a shell.	7.2	More Details
CVE-2021-26724	OS Command Injection vulnerability when changing date settings or hostname using web GUI of Nozomi Networks Guardian and CMC allows authenticated administrators to perform remote code execution. This issue affects: Nozomi Networks Guardian 20.0.7.3 version 20.0.7.3 and prior versions. Nozomi Networks CMC 20.0.7.3 version 20.0.7.3 and prior versions.	7.2	More Details
CVE-2021-26725	Path Traversal vulnerability when changing timezone using web GUI of Nozomi Networks Guardian, CMC allows an authenticated administrator to read-protected system files. This issue affects: Nozomi Networks Guardian 20.0.7.3 version 20.0.7.3 and prior versions. Nozomi Networks CMC 20.0.7.3 version 20.0.7.3 and prior versions.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23340	This affects the package pimcore/pimcore before 6.8.8. A Local FIle Inclusion vulnerability exists in the downloadCsvAction function of the CustomReportController class (bundles/AdminBundle/Controller/Reports/CustomReportController.php). An authenticated user can reach this function with a GET request at the following endpoint: /admin/reports/custom-report/download-csv?exportFile=&91;filename]. Since exportFile variable is not sanitized, an attacker can exploit a local file inclusion vulnerability.	7.1	More Details
CVE-2021-26926	A flaw was found in jasper before 2.0.25. An out of bounds read issue was found in jp2_decode function whic may lead to disclosure of information or program crash.	7.1	More Details
CVE-2020-11203	Stack overflow may occur if GSM/WCDMA broadcast config size received from user is larger than variable length array in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	7.1	More Details
CVE-2020-29075	Acrobat Reader DC versions 2020.013.20066 (and earlier), 2020.001.30010 (and earlier) and 2017.011.30180 (and earlier) are affected by an information exposure vulnerability, that could enable an attacker to get a DNS interaction and track if the user has opened or closed a PDF file when loaded from the filesystem without a prompt. User interaction is required to exploit this vulnerability.	7.1	More Details
CVE-2020-36252	ownCloud Server 10.x before 10.3.1 allows an attacker, who has one outgoing share from a victim, to access any version of any file by sending a request for a predictable ID number.	6.8	More Details
CVE-2020-11286	An Untrusted Pointer Dereference can occur while doing USB control transfers, if multiple requests of different standard request categories like device, interface & endpoint are made together. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.8	More Details
CVE-2020-22475	"Tasks" application version before 9.7.3 is affected by insecure permissions. The VoiceCommandActivity application component allows arbitrary applications on a device to add tasks with no restrictions.	6.8	More Details
CVE-2020-35499	A NULL pointer dereference flaw in Linux kernel versions prior to 5.11 may be seen if sco_sock_getsockopt function in net/bluetooth/sco.c do not have a sanity check for a socket connection, when using BT_SNDMTU/BT_RCVMTU for SCO sockets. This could allow a local attacker with a special user privilege to crash the system (DOS) or leak kernel internal information.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12373	Expired pointer dereference in some Intel(R) Graphics Drivers before version 26.20.100.8141 may allow a privileged user to potentially enable a denial of service via local access.	6.7	More Details
CVE-2020-12374	Buffer overflow in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.47 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-8765	Incorrect default permissions in the installer for the Intel(R) RealSense(TM) DCM may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-8701	Incorrect default permissions in installer for the Intel(R) SSD Toolbox versions before 2/9/2021 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-11198	Key material used for TZ diag buffer encryption and other data related to log buffer is not wiped securely due to improper usage of memset in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	6.7	More Details
CVE-2020-12375	Heap overflow in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.47 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2020-11147	Use after free issue in audio modules while removing and freeing objects during list iteration due to incorrect usage of macro in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile	6.7	More Details
CVE-2021-26686	A remote authenticated SQL Injection vulnerabilitiy was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the web-based management interface API of ClearPass could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass instance. An attacker could exploit this vulnerability to obtain and modify sensitive information in the underlying database.	6.5	More Details
CVE-2021-22553	Any git operation is passed through Jetty and a session is created. No expiry is set for the session and Jetty does not automatically dispose of the session. Over multiple git actions, this can lead to a heap memory exhaustion for Gerrit servers. We recommend upgrading Gerrit to any of the versions listed above.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26685	A remote authenticated SQL Injection vulnerabilitiy was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the web-based management interface API of ClearPass could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass instance. An attacker could exploit this vulnerability to obtain and modify sensitive information in the underlying database.	6.5	More Details
CVE-2021-3405	A flaw was found in libebml before 1.4.2. A heap overflow bug exists in the implementation of EbmlString::ReadData and EbmlUnicodeString::ReadData in libebml.	6.5	More Details
CVE-2021-20252	A flaw was found in Red Hat 3scale API Management Platform 2. The 3scale backend does not perform preventive handling on user-requested date ranges in certain queries allowing a malicious authenticated user to submit a request with a sufficiently large date range to eventually yield an internal server error resulting in denial of service. The highest threat from this vulnerability is to system availability.	6.5	More Details
CVE-2020-22474	In webERP 4.15, the ManualContents.php file allows users to specify the "Language" parameter, which can lead to local file inclusion.	6.5	More Details
CVE-2021-3204	SSRF in the document conversion component of Webware Webdesktop 5.1.15 allows an attacker to read all files from the server.	6.5	More Details
CVE-2020-28463	All versions of package reportlab are vulnerable to Server-side Request Forgery (SSRF) via img tags. In order to reduce risk, use trustedSchemes & trustedHosts (see in Reportlab's documentation) Steps to reproduce by Karan Bamal: 1. Download and install the latest package of reportlab 2. Go to demos -> odyssey -> dodyssey 3. In the text file odyssey.txt that needs to be converted to pdf inject 4. Create a nc listener nc -lp 5000 5. Run python3 dodyssey.py 6. You will get a hit on your nc showing we have successfully proceded to send a server side request 7. dodyssey.py will show error since there is no img file on the url, but we are able to do SSRF	6.5	More Details
CVE-2020-35577	In Endalia Selection Portal before 4.205.0, an Insecure Direct Object Reference (IDOR) allows any authenticated user to download every file uploaded to the platform by changing the value of the file identifier (aka CommonDownload identification number).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1416	Multiple vulnerabilities in the Admin portal of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information. These vulnerabilities are due to improper enforcement of administrator privilege levels for sensitive data. An attacker with read-only administrator access to the Admin portal could exploit these vulnerabilities by browsing to one of the pages that contains sensitive data. A successful exploit could allow the attacker to collect sensitive information regarding the configuration of the system. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2021-1412	Multiple vulnerabilities in the Admin portal of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information. These vulnerabilities are due to improper enforcement of administrator privilege levels for sensitive data. An attacker with read-only administrator access to the Admin portal could exploit these vulnerabilities by browsing to one of the pages that contains sensitive data. A successful exploit could allow the attacker to collect sensitive information regarding the configuration of the system. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2020-24501	Buffer overflow in the firmware for Intel(R) E810 Ethernet Controllers before version 1.4.1.13 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2021-27328	Yeastar NeoGate TG400 91.3.0.3 devices are affected by Directory Traversal. An authenticated user can decrypt firmware and can read sensitive information, such as a password or decryption key.	6.5	More Details
CVE-2021-26559	Improper Access Control on Configurations Endpoint for the Stable API of Apache Airflow allows users with Viewer or User role to get Airflow Configurations including sensitive information even when `[webserver] expose_config` is set to `False` in `airflow.cfg`. This allowed a privilege escalation attack. This issue affects Apache Airflow 2.0.0.	6.5	More Details
CVE-2021-27124	SQL injection in the expertise parameter in search_result.php in Doctor Appointment System v1.0 allows an authenticated patient user to dump the database credentials via a SQL injection attack.	6.5	More Details
CVE-2021-26713	A stack-based buffer overflow in res_rtp_asterisk.c in Sangoma Asterisk before 16.16.1, 17.x before 17.9.2, and 18.x before 18.2.1 and Certified Asterisk before 16.8-cert6 allows an authenticated WebRTC client to cause an Asterisk crash by sending multiple hold/unhold requests in quick succession. This is caused by a signedness comparison mismatch.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35776	A buffer overflow in res_pjsip_diversion.c in Sangoma Asterisk versions 13.38.1, 16.15.1, 17.9.1, and 18.1.1 allows remote attacker to crash Asterisk by deliberately misusing SIP 181 responses.	6.5	More Details
CVE-2020-12668	Jinjava before 2.5.4 allow access to arbitrary classes by calling Java methods on objects passed into a Jinjava context. This could allow for abuse of the application class loader, including Arbitrary File Disclosure.	6.5	More Details
CVE-2021-20445	IBM Maximo for Civil Infrastructure 7.6.2 could allow a user to obtain sensitive information due to insecure storeage of authentication credentials. IBM X-Force ID: 196621.	6.5	More Details
CVE-2021-26682	A remote reflected cross-site scripting (XSS) vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the guest portal interface of ClearPass could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the portal. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the guest portal interface.	6.1	More Details
CVE-2020-19762	Automated Logic Corporation (ALC) WebCTRL System 6.5 and prior allows remote attackers to execute any JavaScript code via a XSS payload for the first parameter in a GET request.	6.1	More Details
CVE-2020-13697	An issue was discovered in RouterNanoHTTPD.java in NanoHTTPD through 2.3.1. The GeneralHandler class implements a basic GET handler that prints debug information as an HTML page. Any web server that extends this class without implementing its own GET handler is vulnerable to reflected XSS, because the GeneralHandler GET handler prints user input passed through the query string without any sanitization.	6.1	More Details
CVE-2021-27403	Askey RTF8115VW BR_SV_g11.11_RTF_TEF001_V6.54_V014 devices allow cgi-bin/te_acceso_router.cgi curWebPage XSS.	6.1	More Details
CVE-2021-27404	Askey RTF8115VW BR_SV_g11.11_RTF_TEF001_V6.54_V014 devices allow injection of a Host HTTP header.	6.1	More Details
CVE-2021-26746	Chamilo 1.11.14 allows XSS via a main/calendar/agenda_list.php?type= URI.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26678	A remote unauthenticated stored cross-site scripting (XSS) vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the web-based management interface of ClearPass could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	6.1	More Details
CVE-2021-20444	IBM Maximo for Civil Infrastructure 7.6.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196620.	6.1	More Details
CVE-2020-36250	In the ownCloud application before 2.15 for Android, the lock protection mechanism can be bypassed by moving the system date/time into the past.	6.1	More Details
CVE-2020-35852	Chatbox is affected by cross-site scripting (XSS). An attacker has to upload any XSS payload with SVG, XML file in Chatbox. There is no restriction on file upload in Chatbox which leads to stored XSS.	6.1	More Details
CVE-2020-35571	An issue was discovered in MantisBT through 2.24.3. In the helper_ensure_confirmed call in manage_custom_field_update.php, the custom field name is not sanitized. This may be problematic depending on CSP settings.	6.1	More Details
CVE-2021-1351	A vulnerability in the web-based interface of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface of the affected service. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected service. An attacker could exploit this vulnerability by persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2021-3189	The slashify package 1.0.0 for Node.js allows open-redirect attacks, as demonstrated by a localhost:3000///example.com/ substring.	6.1	More Details
CVE-2020-2502	This cross-site scripting vulnerability in Photo Station allows remote attackers to inject malicious code. QANP We have already fixed this vulnerability in the following versions of Photo Station. Photo Station 6.0.11 and later	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26716	Modules/input/Views/schedule.php in Emoncms through 10.2.7 allows XSS via the node parameter.	6.1	More Details
CVE-2020-35664	An issue was discovered in Acronis Cyber Protect before 15 Update 1 build 26172. There is cross-site scripting (XSS) in the console.	6.1	More Details
CVE-2021-27214	A Server-side request forgery (SSRF) vulnerability in the ProductConfig servlet in Zoho ManageEngine ADSelfService Plus through 6013 allows a remote unauthenticated attacker to perform blind HTTP requests or perform a Cross-site scripting (XSS) attack against the administrative interface via an HTTP request, a different vulnerability than CVE-2019-3905.	6.1	More Details
CVE-2020-3664	Out of bound read access in hypervisor due to an invalid read access attempt by passing invalid addresses in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	6.0	More Details
CVE-2021-27189	The CIRA Canadian Shield app before 4.0.13 for iOS lacks SSL Certificate Validation.	5.9	More Details
CVE-2021-26906	An issue was discovered in res_pjsip_session.c in Digium Asterisk through 13.38.1; 14.x, 15.x, and 16.x through 16.16.0; 17.x through 17.9.1; and 18.x through 18.2.0, and Certified Asterisk through 16.8-cert5. An SDP negotiation vulnerability in PJSIP allows a remote server to potentially crash Asterisk by sending specific SIP responses that cause an SDP negotiation failure.	5.9	More Details
CVE-2020-24393	TweetStream 2.6.1 uses the library eventmachine in an insecure way that does not have TLS hostname validation. This allows an attacker to perform a man-in-the-middle attack.	5.9	More Details
CVE-2021-27568	An issue was discovered in netplex json-smart-v1 through 2015-10-23 and json-smart-v2 through 2.4. An exception is thrown from a function, but it is not caught, as demonstrated by NumberFormatException. When it is not caught, it may cause programs using the library to crash or expose sensitive information.	5.9	More Details
CVE-2020-24392	In voloko twitter-stream 0.1.10, missing TLS hostname validation allows an attacker to perform a man-in-the-middle attack against users of the library (because eventmachine is misused).	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10254	An issue was discovered in ownCloud before 10.4. An attacker can bypass authentication on a password-protected image by displaying its preview.	5.9	More Details
CVE-2020-25605	Cleartext transmission of sensitive information in Agora Video SDK prior to 3.1 allows a remote attacker to obtain access to audio and video of any ongoing Agora video call through observation of cleartext network traffic.	5.9	More Details
CVE-2020-12363	Improper input validation in some Intel(R) Graphics Drivers for Windows* before version 26.20.100.7212 and before Linux kernel version 5.5 may allow a privileged user to potentially enable a denial of service via local access.	5.5	More Details
CVE-2020-12364	Null pointer reference in some Intel(R) Graphics Drivers for Windows* before version 26.20.100.7212 and before version Linux kernel version 5.5 may allow a privileged user to potentially enable a denial of service via local access.	5.5	More Details
CVE-2020-0524	Improper default permissions in the firmware for the Intel(R) Ethernet I210 Controller series of network adapters before version 3.30 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-23827	Keybase Desktop Client before 5.6.0 on Windows and macOS, and before 5.6.1 on Linux, allows an attacker to obtain potentially sensitive media (such as private pictures) in the Cache and uploadtemps directories. It fails to effectively clear cached pictures, even after deletion via normal methodology within the client, or by utilizing the "Explode message/Explode now" functionality. Local filesystem access is needed by the attacker.	5.5	More Details
CVE-2020-27819	An issue was discovered in libxls before and including 1.6.1 when reading Microsoft Excel files. A NULL pointer dereference vulnerability exists when parsing XLS cells in libxls/xls2csv.c:199. It could allow a remote attacker to cause a denial of service via crafted XLS file.	5.5	More Details
CVE-2020-12361	Use after free in some Intel(R) Graphics Drivers before version 15.33.51.5146 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-24504	Uncontrolled resource consumption in some Intel(R) Ethernet E810 Adapter drivers for Linux before version 1.0.4 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-3407	A flaw was found in mupdf 1.18.0. Double free of object during linearization may lead to memory corruption and other potential consequences.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-18255	HMI/SCADA iFIX (Versions 6.1 and prior) allows a local authenticated user to modify system-wide iFIX configurations through section objects. This may allow privilege escalation.	5.5	More Details
CVE-2021-27550	Polaris Office v9.102.66 is affected by a divide-by-zero error in PolarisOffice.exe and EngineDLL.dll that may cause a local denial of service. To exploit the vulnerability, someone must open a crafted PDF file.	5.5	More Details
CVE-2020-24503	Insufficient access control in some Intel(R) Ethernet E810 Adapter drivers for Linux before version 1.0.4 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2021-26932	An issue was discovered in the Linux kernel 3.2 through 5.10.16, as used by Xen. Grant mapping operations often occur in batch hypercalls, where a number of operations are done in a single hypercall, the success or failure of each one is reported to the backend driver, and the backend driver then loops over the results, performing follow-up actions based on the success or failure of each operation. Unfortunately, when running in PV mode, the Linux backend drivers mishandle this: Some errors are ignored, effectively implying their success from the success of related batch elements. In other cases, errors resulting from one batch element lead to further batch elements not being inspected, and hence successful ones to not be possible to properly unmap upon error recovery. Only systems with Linux backends running in PV mode are vulnerable. Linux backends run in HVM / PVH modes are not vulnerable. This affects arch/*/xen/p2m.c and drivers/xen/gntdev.c.	5.5	More Details
CVE-2021-26933	An issue was discovered in Xen 4.9 through 4.14.x. On Arm, a guest is allowed to control whether memory accesses are bypassing the cache. This means that Xen needs to ensure that all writes (such as the ones during scrubbing) have reached the memory before handing over the page to a guest. Unfortunately, the operation to clean the cache is happening before checking if the page was scrubbed. Therefore there is no guarantee when all the writes will reach the memory.	5.5	More Details
CVE-2021-26927	A flaw was found in jasper before 2.0.25. A null pointer dereference in jp2_decode in jp2_dec.c may lead to program crash and denial of service.	5.5	More Details
CVE-2020-0518	Improper access control in the Intel(R) HD Graphics Control Panel before version 15.40.46.5144 and 15.36.39.5143 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1372	A vulnerability in Cisco Webex Meetings Desktop App and Webex Productivity Tools for Windows could allow an authenticated, local attacker to gain access to sensitive information on an affected system. This vulnerability is due to the unsafe usage of shared memory by the affected software. An attacker with permissions to view system memory could exploit this vulnerability by running an application on the local system that is designed to read shared memory. A successful exploit could allow the attacker to retrieve sensitive information from the shared memory, including usernames, meeting information, or authentication tokens. Note: To exploit this vulnerability, an attacker must have valid credentials on a Microsoft Windows end-user system and must log in after another user has already authenticated with Webex on the same end-user system.	5.5	More Details
CVE-2019-18243	HMI/SCADA iFIX (Versions 6.1 and prior) allows a local authenticated user to modify system-wide iFIX configurations through the registry. This may allow privilege escalation.	5.5	More Details
CVE-2020-24502	Improper input validation in some Intel(R) Ethernet E810 Adapter drivers for Linux before version 1.0.4 and before version 1.4.29.0 for Windows*, may allow an authenticated user to potentially enable a denial of service via local access.	5.5	More Details
CVE-2020-24452	Improper input validation in the Intel(R) SGX Platform Software for Windows* may allow an authenticated user to potentially enable a denial of service via local access.	5.5	More Details
CVE-2020-12365	Untrusted pointer dereference in some Intel(R) Graphics Drivers before versions 15.33.51.5146, 15.45.32.5145, 15.36.39.5144 and 15.40.46.5143 may allow an authenticated user to potentially denial of service via local access.	5.5	More Details
CVE-2020-12370	Untrusted pointer dereference in some Intel(R) Graphics Drivers before version 26.20.100.8141 may allow a privileged user to potentially enable a denial of service via local access.	5.5	More Details
CVE-2020-12372	Unchecked return value in some Intel(R) Graphics Drivers before version 26.20.100.8141 may allow a privileged user to potentially enable a denial of service via local access.	5.5	More Details
CVE-2020-12376	Use of hard-coded key in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.47 may allow authenticated user to potentially enable information disclosure via local access.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26931	An issue was discovered in the Linux kernel 2.6.39 through 5.10.16, as used in Xen. Block, net, and SCSI backends consider certain errors a plain bug, deliberately causing a kernel crash. For errors potentially being at least under the influence of guests (such as out of memory conditions), it isn't correct to assume a plain bug. Memory allocations potentially causing such crashes occur only when Linux is running in PV mode, though. This affects drivers/block/xen-blkback/blkback.c and drivers/xen/xen-scsiback.c.	5.5	More Details
CVE-2020-12386	Out-of-bounds write in some Intel(R) Graphics Drivers before version 15.36.39.5143 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2020-12371	Divide by zero in some Intel(R) Graphics Drivers before version 26.20.100.8141 may allow a privileged user to potentially enable a denial of service via local access.	5.5	More Details
CVE-2020-24448	Uncaught exception in some Intel(R) Graphics Drivers before version 15.33.51.5146 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-27279	MyBB before 1.8.25 allows stored XSS via nested [email] tags with MyCode (aka BBCode).	5.4	More Details
CVE-2021-27370	The Contact page in Monica 2.19.1 allows stored XSS via the Last Name field.	5.4	More Details
CVE-2021-21318	Opencast is a free, open-source platform to support the management of educational audio and video content. In Opencast before version 9.2 there is a vulnerability in which publishing an episode with strict access rules will overwrite the currently set series access. This allows for an easy denial of access for all users without superuser privileges, effectively hiding the series. Access to series and series metadata on the search service (shown in media module and player) depends on the events published which are part of the series. Publishing an event will automatically publish a series and update access to it. Removing an event or republishing the event should do the same. Affected versions of Opencast may not update the series access or remove a published series if an event is being removed. On removal of an episode, this may lead to an access control list for series metadata with broader access rules than the merged access rules of all remaining events, or the series metadata still being available although all episodes of that series have been removed. This problem is fixed in Opencast 9.2.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26544	Livy server version 0.7.0-incubating (only) is vulnerable to a cross site scripting issue in the session name. A malicious user could use this flaw to access logs and results of other users' sessions and run jobs with their privileges. This issue is fixed in Livy 0.7.1-incubating.	5.4	More Details
CVE-2021-20446	IBM Maximo for Civil Infrastructure 7.6.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196622.	5.4	More Details
CVE-2021-22853	The HR Portal of Soar Cloud System fails to manage access control. While obtaining user ID, remote attackers can access sensitive data via a specific data packet, such as user’s login information, further causing the login function not to work.	5.4	More Details
CVE-2021-27368	The Contact page in Monica 2.19.1 allows stored XSS via the First Name field.	5.4	More Details
CVE-2021-27369	The Contact page in Monica 2.19.1 allows stored XSS via the Middle Name field.	5.4	More Details
CVE-2021-27564	A stored XSS issue exists in Appspace 6.2.4. After a user is authenticated and enters an XSS payload under the groups section of the network tab, it is stored as the group name. Whenever another member visits that group, this payload executes.	5.4	More Details
CVE-2020-4933	IBM Jazz Reporting Service 6.0.6.1, 7.0, 7.0.1, and 7.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 191751.	5.4	More Details
CVE-2021-27371	The Contact page in Monica 2.19.1 allows stored XSS via the Description field.	5.4	More Details
CVE-2020-26609	fastadmin V1.0.0.20200506_beta contains a cross-site scripting (XSS) vulnerability which may allow an attacker to obtain administrator credentials to log in to the background.	5.4	More Details
CVE-2021-27559	The Contact page in Monica 2.19.1 allows stored XSS via the Nickname field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35592	Pi-hole 5.0, 5.1, and 5.1.1 allows XSS via the Options header to the admin/ URI. A remote user is able to inject arbitrary web script or HTML due to incorrect sanitization of user-supplied data and achieve a Reflected Cross-Site Scripting attack against other users and steal the session cookie.	5.4	More Details
CVE-2020-35591	Pi-hole 5.0, 5.1, and 5.1.1 allows Session Fixation. The application does not generate a new session cookie after the user is logged in. A malicious user is able to create a new session cookie value and inject it to a victim. After the victim logs in, the injected cookie becomes valid, giving the attacker access to the user's account through the active session.	5.4	More Details
CVE-2021-20653	Calsos CSDJ (CSDJ-B 01.08.00 and earlier, CSDJ-H 01.08.00 and earlier, CSDJ-D 01.08.00 and earlier, and CSDJ-A 03.08.00 and earlier) allows remote attackers to bypass access restriction and to obtain unauthorized historical data without access privileges via unspecified vectors.	5.3	More Details
CVE-2021-26697	The lineage endpoint of the deprecated Experimental API was not protected by authentication in Airflow 2.0.0. This allowed unauthenticated users to hit that endpoint. This is low-severity issue as the attacker needs to be aware of certain parameters to pass to that endpoint and even after can just get some metadata about a DAG and a Task. This issue affects Apache Airflow 2.0.0.	5.3	More Details
CVE-2021-27515	url-parse before 1.5.0 mishandles certain uses of backslash such as http:\/ and interprets the URI as a relative path.	5.3	More Details
CVE-2021-1378	A vulnerability in the SSH service of the Cisco StarOS operating system could allow an unauthenticated, remote attacker to cause an affected device to stop processing traffic, resulting in a denial of service (DoS) condition. The vulnerability is due to a logic error that may occur under specific traffic conditions. An attacker could exploit this vulnerability by sending a series of crafted packets to an affected device. A successful exploit could allow the attacker to prevent the targeted service from receiving any traffic, which would lead to a DoS condition on the affected device.	5.3	More Details
CVE-2020-7120	A local authenticated buffer overflow vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in ClearPass OnGuard could allow local authenticated users to cause a buffer overflow condition. A successful exploit could allow a local attacker to execute arbitrary code within the context the binary is running in, which is a lower privileged account.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20256	A flaw was found in Red Hat Satellite. The BMC interface exposes the password through the API to an authenticated local attacker with view_hosts permission. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	5.3	More Details
CVE-2021-27351	The Terminate Session feature in the Telegram application through 7.2.1 for Android, and through 2.4.7 for Windows and UNIX, fails to invalidate a recently active session.	5.3	More Details
CVE-2021-27583	In Directus 8.x through 8.8.1, an attacker can discover whether a user is present in the database through the password reset feature. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	5.3	More Details
CVE-2021-27375	Traefik before 2.4.5 allows the loading of IFRAME elements from other domains.	5.3	More Details
CVE-2021-26595	In Directus 8.x through 8.8.1, an attacker can learn sensitive information such as the version of the CMS, the PHP version used by the site, and the name of the DBMS, simply by view the result of the api-aa, called automatically upon a connection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	5.3	More Details
CVE-2021-22113	Applications using the “Sensitive Headers” functionality in Spring Cloud Netflix Zuul 2.2.6.RELEASE and below may be vulnerable to bypassing the “Sensitive Headers” restriction when executing requests with specially constructed URLs. Applications that use Spring Security's StrictHttpFirewall (enabled by default for all URLs) are not affected by the vulnerability, as they reject requests that allow bypassing.	5.3	More Details
CVE-2020-29453	The CachingResourceDownloadRewriteRule class in Jira Server and Jira Data Center before version 8.5.11, from 8.6.0 before 8.13.3, and from 8.14.0 before 8.15.0 allowed unauthenticated remote attackers to read arbitrary files within WEB-INF and META-INF directories via an incorrect path access check.	5.3	More Details
CVE-2020-29448	The ConfluenceResourceDownloadRewriteRule class in Confluence Server and Confluence Data Center before version 6.13.18, from 6.14.0 before 7.4.6, and from 7.5.0 before 7.8.3 allowed unauthenticated remote attackers to read arbitrary files within WEB-INF and META-INF directories via an incorrect path access check.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27549	Genymotion Desktop through 3.2.0 leaks the host's clipboard data to the Android application by default. NOTE: the vendor's position is that this is intended behavior that can be changed through the Settings > Device screen	5.3	More Details
CVE-2020-24458	Incomplete cleanup in some Intel(R) PROSet/Wireless WiFi and Killer (TM) drivers before version 22.0 may allow a privileged user to potentially enable information disclosure and denial of service via adjacent access.	5.2	More Details
CVE-2021-23339	This affects all versions before 10.1.14 and from 10.2.0 to 10.2.4 of package com.typesafe.akka:akka-http-core. It allows multiple Transfer-Encoding headers.	5.0	More Details
CVE-2020-36232	The MessageBundleWhiteList class of atlassian-gadgets before version 4.2.37, from version 4.3.0 before 4.3.14, from version 4.3.2.0 before 4.3.2.4, from version 4.4.0 before 4.4.12, and from version 5.0.0 before 5.0.1 allowed unexpected DNS lookups and requests to arbitrary services as it incorrectly obtained application base url information from the executing http request which could be attacker controlled.	5.0	More Details
CVE-2021-3271	PressBooks 5.17.3 contains a cross-site scripting (XSS). Stored XSS can be submitted via the Book Info's Long Description Body, and all actions to open or preview the books page will result in the triggering the stored XSS.	4.8	More Details
CVE-2021-20220	A flaw was found in Undertow. A regression in the fix for CVE-2020-10687 was found. HTTP request smuggling related to CVE-2017-2666 is possible against HTTP/1.x and HTTP/2 due to permitting invalid characters in an HTTP request. This flaw allows an attacker to poison a web-cache, perform an XSS attack, or obtain sensitive information from request other than their own. The highest threat from this vulnerability is to data confidentiality and integrity.	4.8	More Details
CVE-2021-22701	A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.	4.5	More Details
CVE-2020-24493	Insufficient access control in the firmware for the Intel(R) 700-series of Ethernet Controllers before version 8.0 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24496	Insufficient input validation in the firmware for Intel(R) 722 Ethernet Controllers before version 1.4.3 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2020-0525	Improper access control in firmware for the Intel(R) Ethernet I210 Controller series of network adapters before version 3.30 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2020-24494	Insufficient access control in the firmware for the Intel(R) 722 Ethernet Controllers before version 1.4.3 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2020-24480	Out-of-bounds write in the Intel(R) XTU before version 6.5.3.25 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2020-0522	Improper initialization in the firmware for the Intel(R) Ethernet I210 Controller series of network adapters before version 3.30 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2020-24495	Insufficient access control in the firmware for the Intel(R) 700-series of Ethernet Controllers before version 7.3 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2020-24497	Insufficient Access Control in the firmware for Intel(R) E810 Ethernet Controllers before version 1.4.1.13 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2020-24491	Debug message containing addresses of memory transactions in some Intel(R) 10th Generation Core Processors supporting SGX may allow a privileged user to potentially enable information disclosure via local access.	4.4	More Details
CVE-2020-0523	Improper access control in the firmware for the Intel(R) Ethernet I210 Controller series of network adapters before version 3.30 may potentially allow a privileged user to enable a denial of service via local access.	4.4	More Details
CVE-2020-24505	Insufficient input validation in the firmware for the Intel(R) 700-series of Ethernet Controllers before version 7.3 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2020-24498	Buffer overflow in the firmware for Intel(R) E810 Ethernet Controllers before version 1.4.1.13 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24500	Buffer overflow in the firmware for Intel(R) E810 Ethernet Controllers before version 1.4.1.13 may allow a privileged user to potentially enable a denial of service via local access.	4.4	More Details
CVE-2020-24492	Insufficient access control in the firmware for the Intel(R) 722 Ethernet Controllers before version 1.5 may allow a privileged user to potentially enable a denial of service via local access.	4.4	More Details
CVE-2021-21323	Brave is an open source web browser with a focus on privacy and security. In Brave versions 1.17.73-1.20.103, the CNAME adblocking feature added in Brave 1.17.73 accidentally initiated DNS requests that bypassed the Brave Tor proxy. Users with adblocking enabled would leak DNS requests from Tor windows to their DNS provider. (DNS requests that were not initiated by CNAME adblocking would go through Tor as expected.) This is fixed in Brave version 1.20.108	4.3	More Details
CVE-2021-20229	A flaw was found in PostgreSQL in versions before 13.2. This flaw allows a user with SELECT privilege on one column to craft a special query that returns all columns of the table. The highest threat from this vulnerability is to confidentiality.	4.3	More Details
CVE-2020-8297	Nextcloud Deck before 1.0.2 suffers from an insecure direct object reference (IDOR) vulnerability that permits users with a duplicate user identifier to access deck data of a previous deleted user.	4.3	More Details
CVE-2020-4953	IBM Planning Analytics 2.0 could allow a remote authenticated attacker to obtain information about an organization's internal structure by exposing sensitive information in HTTP repsonses. IBM X-Force ID: 192029.	4.3	More Details
CVE-2021-3339	ModernFlow before 1.3.00.208 does not constrain web-page access to members of a security group, as demonstrated by the Search Screen and the Profile Screen.	4.3	More Details
CVE-2020-36248	The ownCloud application before 2.15 for Android allows attackers to use adb to include a PIN preferences value in a backup archive, and consequently bypass the PIN lock feature by restoring from this archive.	3.9	More Details
CVE-2021-22174	Crash in USB HID dissector in Wireshark 3.4.0 to 3.4.2 allows denial of service via packet injection or crafted capture file	3.7	More Details
CVE-2021-22173	Memory leak in USB HID dissector in Wireshark 3.4.0 to 3.4.2 allows denial of service via packet injection or crafted capture file	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8902	Rendertron versions prior to 3.0.0 are are susceptible to a Server-Side Request Forgery (SSRF) attack. An attacker can use a specially crafted webpage to force a rendertron headless chrome process to render internal sites it has access to, and display it as a screenshot. Suggested mitigations are to upgrade your rendertron to version 3.0.0, or, if you cannot update, to secure the infrastructure to limit the headless chrome's access to your internal domain.	3.5	More Details
CVE-2020-36251	ownCloud Server before 10.3.0 allows an attacker, who has received non-administrative access to a group share, to remove everyone else's access to that share.	3.5	More Details
CVE-2020-27768	In ImageMagick, there is an outside the range of representable values of type 'unsigned int' at MagickCore/quantum-private.h. This flaw affects ImageMagick versions prior to 7.0.9-0.	3.3	More Details
CVE-2020-28431	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-27785	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-29074. Reason: This candidate is a reservation duplicate of CVE-2020-29074. Notes: All CVE users should reference CVE-2020-29074 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-20242	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-20176. Reason: This candidate is a reservation duplicate of CVE-2021-20176. Notes: All CVE users should reference CVE-2021-20176 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2020-28430	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-28432	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details