SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 09 December 2020

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2017-14451	An exploitable out-of-bounds read vulnerability exists in libevm (Ethereum Virtual Machine) of CPP-Ethereum. A specially crafted smart contract code can cause an out-of-bounds read which can subsequently trigger an out-of-bounds write resulting in remote code execution. An attacker can create/send malicious smart contract to trigger this vulnerability.	10.0	More Details
CVE-2020-14260	HCL Domino is susceptible to a Buffer Overflow vulnerability in DXL due to improper validation of user input. A successful exploit could enable an attacker to crash Domino or execute attacker-controlled code on the server system.	9.8	More Details
CVE-2020-29575	The official elixir Docker images before 1.8.0-alpine (Alpine specific) contain a blank password for a root user. Systems using the elixir Linux Docker container deployed by affected versions of the Docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29597	IncomCMS 2.0 has a modules/uploader/showcase/script.php insecure file upload vulnerability. This vulnerability allows unauthenticated attackers to upload files into the server.	9.8	More Details
CVE-2020-29600	In AWStats through 7.7, cgi-bin/awstats.pl?config= accepts an absolute pathname, even though it was intended to only read a file in the /etc/awstats/awstats.conf format. NOTE: this issue exists because of an incomplete fix for CVE-2017-1000501.	9.8	More Details
CVE-2020-17531	A Java Serialization vulnerability was found in Apache Tapestry 4. Apache Tapestry 4 will attempt to deserialize the "sp" parameter even before invoking the page's validate method, leading to deserialization without authentication. Apache Tapestry 4 reached end of life in 2008 and no update to address this issue will be released. Apache Tapestry 5 versions are not vulnerable to this issue. Users of Apache Tapestry 4 should upgrade to the latest Apache Tapestry 5 version.	9.8	More Details
CVE-2020-25889	Online Bus Booking System Project Using PHP/MySQL version 1.0 has SQL injection via the login page. By placing SQL injection payload on the login page attackers can bypass the authentication and can gain the admin privilege.	9.8	More Details
CVE-2020-29578	The official piwik Docker images before fpm-alpine (Alpine specific) contain a blank password for a root user. Systems using the Piwik Docker container deployed by affected versions of the Docker image may allow an remote attacker to achieve root access.	9.8	More Details
CVE-2020-29564	The official Consul Docker images 0.7.1 through 1.4.2 contain a blank password for a root user. System using the Consul Docker container deployed by affected versions of the Docker image may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-29576	The official eggdrop Docker images before 1.8.4rc2 contain a blank password for a root user. Systems using the Eggdrop Docker container deployed by affected versions of the Docker image may allow an remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-5800	The Eat Spray Love mobile app for both iOS and Android contains logic that allows users to bypass authentication and retrieve or modify information that they would not normally have access to.	9.8	More Details
CVE-2020-29577	The official znc docker images before 1.7.1-slim contain a blank password for a root user. Systems using the znc docker container deployed by affected versions of the Docker image may allow an remote attacker to achieve root access with a blank password.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29579	The official Express Gateway Docker images before 1.14.0 contain a blank password for a root user. Systems using the Express Gateway Docker container deployed by affected versions of the Docker image may allow an remote attacker to achieve root access.	9.8	More Details
CVE-2020-29580	The official storm Docker images before 1.2.1 contain a blank password for a root user. Systems using the Storm Docker container deployed by affected versions of the Docker image may allow an remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-29581	The official spiped docker images before 1.5-alpine contain a blank password for a root user. Systems using the spiped docker container deployed by affected versions of the docker image may allow an remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-29601	The official notary docker images before signer-0.6.1-1 contain a blank password for a root user. System using the notary docker container deployed by affected versions of the docker image may allow an remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-29602	The official irssi docker images before 1.1-alpine (Alpine specific) contain a blank password for a root user. System using the irssi docker container deployed by affected versions of the Docker image may allow an remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-29595	PlugIns\IDE_ACDStd.apl in ACDSee Photo Studio Studio Professional 2021 14.0 Build 1705 has a User Mode Write AV starting at IDE_ACDStd!JPEGTransW+0x00000000000031aa.	9.8	More Details
CVE-2020-5799	The Eat Spray Love mobile app for both iOS and Android contains a backdoor account that, when modified, allowed privileged access to restricted functionality and to other users' data.	9.8	More Details
CVE-2020-6018	Valve's Game Networking Sockets prior to version v1.2.0 improperly handles long encrypted messages in function AES_GCM_DecryptContext::Decrypt() when compiled using libsodium, leading to a Stack-Based Buffer Overflow and resulting in a memory corruption and possibly even a remote code execution.	9.8	More Details
CVE-2020-29282	SQL injection vulnerability in BloodX 1.0 allows attackers to bypass authentication.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7199	A security vulnerability has been identified in the HPE Edgeline Infrastructure Manager, also known as HPE Edgeline Infrastructure Management Software. The vulnerability could be remotely exploited to bypass remote authentication leading to execution of arbitrary commands, gaining privileged access, causing denial of service, and changing the configuration.	9.8	More Details
CVE-2020-28272	Prototype pollution vulnerability in 'keyget' versions 1.0.0 through 2.2.0 allows attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2020-28273	Prototype pollution vulnerability in 'set-in' versions 1.0.0 through 2.0.0 allows attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2020-29389	The official Crux Linux Docker images 3.0 through 3.4 contain a blank password for a root user. System using the Crux Linux Docker container deployed by affected versions of the Docker image may allow an attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-29279	PHP remote file inclusion in the assign_resume_tpl method in Application/Common/Controller/BaseController.class.php in 74CMS before 6.0.48 allows remote code execution.	9.8	More Details
CVE-2020-29280	The Victor CMS v1.0 application is vulnerable to SQL injection via the 'search' parameter on the search.php page.	9.8	More Details
CVE-2020-29283	An SQL injection vulnerability was discovered in Online Doctor Appointment Booking System PHP and Mysql via the q parameter to getuser.php.	9.8	More Details
CVE-2020-25462	Heap buffer overflow in the fxCheckArrowFunction function at moddable/xs/sources/xsSyntaxical.c:3562 in Moddable SDK before OS200903.	9.8	More Details
CVE-2020-29284	The file view-chair-list.php in Multi Restaurant Table Reservation System 1.0 does not perform input validation on the table_id parameter which allows unauthenticated SQL Injection. An attacker can send malicious input in the GET request to /dashboard/view-chair-list.php?table_id= to trigger the vulnerability.	9.8	More Details
CVE-2020-29285	SQL injection vulnerability was discovered in Point of Sales in PHP/PDO 1.0, which can be exploited via the id parameter to edit_category.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29287	An SQL injection vulnerability was discovered in Car Rental Management System v1.0 can be exploited via the id parameter in view_car.php or the car_id parameter in booking.php.	9.8	More Details
CVE-2020-29288	An SQL injection vulnerability was discovered in Gym Management System In manage_user.php file, GET parameter 'id' is vulnerable.	9.8	More Details
CVE-2020-6017	Valve's Game Networking Sockets prior to version v1.2.0 improperly handles long unreliable segments in function SNP_ReceiveUnreliableSegment() when configured to support plain-text messages, leading to a Heap-Based Buffer Overflow and resulting in a memory corruption and possibly even a remote code execution.	9.8	More Details
CVE-2020-2320	Jenkins Plugin Installation Manager Tool 2.1.3 and earlier does not verify plugin downloads.	9.8	More Details
CVE-2020-28274	Prototype pollution vulnerability in 'deepref' versions 1.1.1 through 1.2.1 allows attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-13531	A use-after-free vulnerability exists in a way Pixar OpenUSD 20.08 processes reference paths textual USD files. A specially crafted file can trigger the reuse of a freed memory which can result in further memory corruption and arbitrary code execution. To trigger this vulnerability, the victim needs to open an attacker-provided malformed file.	8.8	More Details
CVE-2020-9947	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, Safari 14.0. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-27151	An issue was discovered in Kata Containers through 1.11.3 and 2.x through 2.0-rc1. The runtime will execute binaries given using annotations without any kind of validation. Someone who is granted access rights to a cluster will be able to have kata-runtime execute arbitrary binaries as root on the worker nodes.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9950	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, tvOS 14.0, Safari 14.0, iOS 14.0 and iPadOS 14.0. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2020-25629	A vulnerability was found in Moodle where users with "Log in as" capability in a course context (typically, course managers) may gain access to some site administration capabilities by "logging in as" a System manager. This affects 3.9 to 3.9.1, 3.8 to 3.8.4, 3.7 to 3.7.7, 3.5 to 3.5.13 and earlier unsupported versions. This is fixed in 3.9.2, 3.8.5, 3.7.8 and 3.5.14.	8.8	More Details
CVE-2017-2910	An exploitable Out-of-bounds Write vulnerability exists in the xls_addCell function of libxls 2.0. A specially crafted xls file can cause a memory corruption resulting in remote code execution. An attacker can send malicious xls file to trigger this vulnerability.	8.8	More Details
CVE-2020-27906	Multiple integer overflows were addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1. A remote attacker may be able to cause unexpected application termination or heap corruption.	8.8	More Details
CVE-2020-13543	A code execution vulnerability exists in the WebSocket functionality of Webkit WebKitGTK 2.30.0. A specially crafted web page can trigger a use-after-free vulnerability which can lead to remote code execution. An attacker can get a user to visit a webpage to trigger this vulnerability.	8.8	More Details
CVE-2020-13584	An exploitable use-after-free vulnerability exists in WebKitGTK browser version 2.30.1 x64. A specially crafted HTML web page can cause a use-after-free condition, resulting in a remote code execution. The victim needs to visit a malicious web site to trigger this vulnerability.	8.8	More Details
CVE-2020-29458	Textpattern CMS 4.6.2 allows CSRF via the prefs subsystem.	8.8	More Details
CVE-2020-14339	A flaw was found in libvirt, where it leaked a file descriptor for `/dev/mapper/control` into the QEMU process. This file descriptor allows for privileged operations to happen against the device-mapper on the host. This flaw allows a malicious guest user or process to perform operations outside of their standard permissions, potentially causing serious damage to the host operating system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13525	The sort parameter in the download page /sysworkflow/en/neoclassic/reportTables/reportTables_Ajax is vulnerable to SQL injection in ProcessMaker 3.4.11. A specially crafted HTTP request can cause an SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2020-25693	A flaw was found in CImg in versions prior to 2.9.3. Integer overflows leading to heap buffer overflows in load_pnm() can be triggered by a specially crafted input file processed by CImg, which can lead to an impact to application availability or data integrity.	8.1	More Details
CVE-2020-14305	An out-of-bounds memory write flaw was found in how the Linux kernel's Voice Over IP H.323 connection tracking functionality handled connections on ipv6 port 1720. This flaw allows an unauthenticated remote user to crash the system, causing a denial of service. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	8.1	More Details
CVE-2020-2321	A cross-site request forgery (CSRF) vulnerability in Jenkins Shelve Project Plugin 3.0 and earlier allows attackers to shelve, unshelve, or delete a project.	8.1	More Details
CVE-2020-28251	NETSCOUT AirMagnet Enterprise 11.1.4 build 37257 and earlier has a sensor escalated privileges vulnerability that can be exploited to provide someone with administrative access to a sensor, with credentials to invoke a command to provide root access to the operating system. The attacker must complete a straightforward password-cracking exercise.	8.1	More Details
CVE-2020-23740	In DriverGenius 9.61.5480.28 there is a local privilege escalation vulnerability in the driver wizard, attackers can use constructed programs to increase user privileges.	7.8	More Details
CVE-2020-29534	An issue was discovered in the Linux kernel before 5.9.3. io_uring takes a non-refcounted reference to the files_struct of the process that submitted a request, causing execve() to incorrectly optimize unshare_fd(), aka CID-0f2122045b94.	7.8	More Details
CVE-2020-6021	Check Point Endpoint Security Client for Windows before version E84.20 allows write access to the directory from which the installation repair takes place. Since the MS Installer allows regular users to run the repair, an attacker can initiate the installation repair and place a specially crafted DLL in the repair folder which will run with the Endpoint client's privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9954	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in watchOS 7.0, tvOS 14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave, iOS 14.0 and iPadOS 14.0. Playing a malicious audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-10003	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A local attacker may be able to elevate their privileges.	7.8	More Details
CVE-2020-29599	ImageMagick before 6.9.11-40 and 7.x before 7.0.10-40 mishandles the -authenticate option, which allows setting a password for password-protected PDF files. The user-controlled password was not properly escaped/sanitized and it was therefore possible to inject additional shell commands via coders/pdf.c.	7.8	More Details
CVE-2020-9949	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, macOS Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra, tvOS 14.0. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-13542	A local privilege elevation vulnerability exists in the file system permissions of LogicalDoc 8.5.1 installation. Depending on the vector chosen, an attacker can either replace the service binary or replace DLL files loaded by the service, both which get executed by a service thus executing arbitrary commands with System privileges.	7.8	More Details
CVE-2020-10016	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-10004	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2020-10010	A path handling issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A local attacker may be able to elevate their privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10011	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 14.2 and iPadOS 14.2, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2020-10013	A logic issue was addressed with improved state management. This issue is fixed in tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-28175	There is a local privilege escalation vulnerability in Alfredo Milani Comparetti SpeedFan 4.52. Attackers can use constructed programs to increase user privileges	7.8	More Details
CVE-2020-14351	A flaw was found in the Linux kernel. A use-after-free memory flaw was found in the perf subsystem allowing a local attacker with permission to monitor perf events to corrupt memory and possibly escalate privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2020-14381	A flaw was found in the Linux kernel's futex implementation. This flaw allows a local attacker to corrupt system memory or escalate their privileges when creating a futex on a filesystem that is about to be unmounted. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	7.8	More Details
CVE-2020-23735	In Saibo Cyber Game Accelerator 3.7.9 there is a local privilege escalation vulnerability. Attackers can use the constructed program to increase user privileges	7.8	More Details
CVE-2020-9247	There is a buffer overflow vulnerability in several Huawei products. The system does not sufficiently validate certain configuration parameter which is passed from user that would cause buffer overflow. The attacker should trick the user into installing and running a malicious application with a high privilege, successful exploit may cause code execution. Affected product include Huawei HONOR 20 PRO, Mate 20, Mate 20 Pro, Mate 20 X, P30, P30 Pro, Hima-L29C, Laya-AL00EP, Princeton-AL10B, Tony-AL00B, Yale-L61A, Yale-TL00B and YaleP-AL10B.	7.8	More Details
CVE-2020-5798	inSync Client installer for macOS versions v6.8.0 and prior could allow an attacker to gain privileges of a root user from a lower privileged user due to improper integrity checks and directory permissions.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9965	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-27910	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-27918	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, Safari 14.0.1, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution.	7.8	More Details
CVE-2020-27932	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-27766	A flaw was found in ImageMagick in MagickCore/statistic.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned long`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.8-69.	7.8	More Details
CVE-2020-27930	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. Processing a maliciously crafted font may lead to arbitrary code execution.	7.8	More Details
CVE-2020-27927	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted font file may lead to arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27926	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 14.2 and iPadOS 14.2. Processing maliciously crafted web content may lead to arbitrary code execution.	7.8	More Details
CVE-2020-27917	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing maliciously crafted web content may lead to code execution.	7.8	More Details
CVE-2020-27916	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9966	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-27912	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2020-27911	An integer overflow was addressed through improved input validation. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2020-28950	The installer of Kaspersky Anti-Ransomware Tool (KART) prior to KART 4.0 Patch C was vulnerable to a DLL hijacking attack that allowed an attacker to elevate privileges during installation process.	7.8	More Details
CVE-2020-27909	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-10017	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. Processing a maliciously crafted audio file may lead to arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9972	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 14.0 and iPadOS 14.0. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2020-9981	A use after free issue was addressed with improved memory management. This issue is fixed in watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0, macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-9996	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A malicious application may be able to elevate privileges.	7.8	More Details
CVE-2020-13493	A heap overflow vulnerability exists in Pixar OpenUSD 20.05 when the software parses compressed sections in binary USD files. A specially crafted USDC file format path jumps decompression heap overflow in a way path jumps are processed. To trigger this vulnerability, the victim needs to open an attacker-provided malformed file.	7.8	More Details
CVE-2020-9999	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iTunes for Windows 12.10.9. Processing a maliciously crafted text file may lead to arbitrary code execution.	7.8	More Details
CVE-2020-27903	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Big Sur 11.0.1. An application may be able to gain elevated privileges.	7.8	More Details
CVE-2020-27904	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-27905	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A malicious application may be able to execute arbitrary code with system privileges.	7.8	More Details
CVE-2020-26246	Pimcore is an open source digital experience platform. In Pimcore before version 6.8.5 it is possible to modify & create website settings without having the appropriate permissions.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26254	omniauth-apple is the OmniAuth strategy for "Sign In with Apple" (RubyGem omniauth-apple). In omniauth-apple before version 1.0.1 attackers can fake their email address during authentication. This vulnerability impacts applications using the omniauth-apple strategy of OmniAuth and using the info.email field of OmniAuth's Auth Hash Schema for any kind of identification. The value of this field may be set to any value of the attacker's choice including email addresses of other users. Applications not using info.email for identification but are instead using the uid field are not impacted in the same manner. Note, these applications may still be negatively affected if the value of info.email is being used for other purposes. Applications using affected versions of omniauth-apple are advised to upgrade to omniauth-apple version 1.0.1 or later.	7.7	More Details
CVE-2020-5675	Out-of-bounds read vulnerability in GT21 model of GOT2000 series (GT2107-WTBD V01.39.000 and earlier, GT2107-WTSD V01.39.000 and earlier, GT2104-RTBD V01.39.000 and earlier, GT2104-PMBD V01.39.000 and earlier, and GT2103-PMBD V01.39.000 and earlier), GS21 model of GOT series (GS2110-WTBD V01.39.000 and earlier, GS2107-WTBD V01.39.000 and earlier, GS2110-WTBD-N V01.39.000 and earlier, and GS2107-WTBD-N V01.39.000 and earlier), and Tension Controller LE7-40GU-L series (LE7-40GU-L Screen package data for CC-Link IEF Basic V1.00, LE7-40GU-L Screen package data for MODBUS/TCP V1.00, and LE7-40GU-L Screen package data for SLMP V1.00) allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted packet. As a result, deterioration of communication performance or a denial-of-service (DoS) condition of the TCP communication functions of the products may occur.	7.5	More Details
CVE-2020-25630	A vulnerability was found in Moodle where the decompressed size of zip files was not checked against available user quota before unzipping them, which could lead to a denial of service risk. This affects versions 3.9 to 3.9.1, 3.8 to 3.8.4, 3.7 to 3.7.7, 3.5 to 3.5.13 and earlier unsupported versions. Fixed in 3.9.2, 3.8.5, 3.7.8 and 3.5.14.	7.5	More Details
CVE-2020-25465	Null Pointer Dereference. in xObjectBindingFromExpression at moddable/xs/sources/xsSyntaxical.c:3419 in Moddable SDK before OS200908 causes a denial of service (SEGV).	7.5	More Details
CVE-2020-29529	HashiCorp go-slug up to 0.4.3 did not fully protect against directory traversal while unpacking tar archives, and protections could be bypassed with specific constructions of multiple symlinks. Fixed in 0.5.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25692	A NULL pointer dereference was found in OpenLDAP server and was fixed in openldap 2.4.55, during a request for renaming RDNs. An unauthenticated attacker could remotely crash the slapd process by sending a specially crafted request, causing a Denial of Service.	7.5	More Details
CVE-2020-29573	sysdeps/i386/ldbl2mpn.c in the GNU C Library (aka glibc or libc6) before 2.23 on x86 targets has a stack-based buffer overflow if the input to any of the printf family of functions is an 80-bit long double with a non-canonical bit pattern, as seen when passing a \x00\x04\x00\x00\x00\x00\x00\x00\x00\x04 value to sprintf. NOTE: the issue does not affect glibc by default in 2016 or later (i.e., 2.23 or later) because of commits made in 2015 for inlining of C99 math functions through use of GCC built-ins. In other words, the reference to 2.23 is intentional despite the mention of "Fixed for glibc 2.33" in the 26649 reference.	7.5	More Details
CVE-2020-25464	Heap buffer overflow at moddable/xs/sources/xsDebug.c in Moddable SDK before before 20200903. The top stack frame is only partially initialized because the stack overflowed while creating the frame. This leads to a crash in the code sending the stack frame to the debugger.	7.5	More Details
CVE-2020-17527	While investigating bug 64830 it was discovered that Apache Tomcat 10.0.0-M1 to 10.0.0-M9, 9.0.0-M1 to 9.0.39 and 8.5.0 to 8.5.59 could re-use an HTTP request header value from the previous stream received on an HTTP/2 connection for the request associated with the subsequent stream. While this would most likely lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak between requests.	7.5	More Details
CVE-2020-25463	Invalid Memory Access in fxUTF8Decode at moddable/xs/sources/xsCommon.c:916 in Moddable SDK before OS200908 causes a denial of service (SEGV).	7.5	More Details
CVE-2020-25461	Invalid Memory Access in the fxProxyGetter function in moddable/xs/sources/xsProxy.c in Moddable SDK before OS200908 causes a denial of service (SEGV).	7.5	More Details
CVE-2020-29540	API calls in the Translation API feature in Systran Pure Neural Server before 9.7.0 allow a threat actor to use the Systran Pure Neural Server as a Denial-of-Service proxy by sending a large amount of translation requests to a destination host on any given TCP port regardless of whether a web service is running on the destination port.	7.5	More Details
CVE-2020-2322	Jenkins Chaos Monkey Plugin 0.3 and earlier does not perform permission checks in several HTTP endpoints, allowing attackers with Overall/Read permission to generate load and to generate memory leaks.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9991	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, iCloud for Windows 7.21, tvOS 14.0. A remote attacker may be able to cause a denial of service.	7.5	More Details
CVE-2020-27813	An integer overflow vulnerability exists with the length of websocket frames received via a websocket connection. An attacker would use this flaw to cause a denial of service attack on an HTTP Server allowing websocket connections.	7.5	More Details
CVE-2020-5423	CAPI (Cloud Controller) versions prior to 1.101.0 are vulnerable to a denial-of-service attack in which an unauthenticated malicious attacker can send specially-crafted YAML files to certain endpoints, causing the YAML parser to consume excessive CPU and RAM.	7.5	More Details
CVE-2020-12524	Uncontrolled Resource Consumption can be exploited to cause the Phoenix Contact HMIs BTP 2043W, BTP 2070W and BTP 2102W in all versions to become unresponsive and not accurately update the display content (Denial of Service).	7.5	More Details
CVE-2020-5676	GROWI v4.1.3 and earlier allow remote attackers to obtain information which is not allowed to access via unspecified vectors.	7.5	More Details
CVE-2020-5680	Improper input validation vulnerability in EC-CUBE versions from 3.0.5 to 3.0.18 allows a remote attacker to cause a denial-of-service (DoS) condition via unspecified vector.	7.5	More Details
CVE-2020-6111	An exploitable denial-of-service vulnerability exists in the IPv4 functionality of Allen-Bradley MicroLogix 1100 Programmable Logic Controller Systems Series B FRN 16.000, Series B FRN 15.002, Series B FRN 15.000, Series B FRN 14.000, Series B FRN 13.000, Series B FRN 12.000, Series B FRN 11.000 and Series B FRN 10.000. A specially crafted packet can cause a major error, resulting in a denial of service. An attacker can send a malicious packet to trigger this vulnerability.	7.5	More Details
CVE-2020-28937	OpenClinic version 0.8.2 is affected by a missing authentication vulnerability that allows unauthenticated users to access any patient's medical test results, possibly resulting in disclosure of Protected Health Information (PHI) stored in the application, via a direct request for the /tests/ URI.	7.5	More Details
CVE-2020-2324	Jenkins CVS Plugin 2.16 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27408	OpenSIS Community Edition through 7.6 is affected by incorrect access controls for the file ResetUserInfo.php that allow an unauthenticated attacker to change the password of arbitrary users.	7.5	More Details
CVE-2020-25649	A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity.	7.5	More Details
CVE-2020-28946	An improper webserver configuration on Plum IK-401 devices with firmware before 1.02 allows an attacker (with network access to the device) to obtain the configuration file, including hashed credential data. Successful exploitation could allow access to hashed credential data with a single unauthenticated GET request.	7.5	More Details
CVE-2020-27778	A flaw was found in Poppler in the way certain PDF files were converted into HTML. A remote attacker could exploit this flaw by providing a malicious PDF file that, when processed by the 'pdftohtml' program, would crash the application causing a denial of service.	7.5	More Details
CVE-2020-25638	A flaw was found in hibernate-core in versions prior to and including 5.4.23.Final. A SQL injection in the implementation of the JPA Criteria API can permit unsanitized literals when a literal is used in the SQL comments of the query. This flaw could allow an attacker to access unauthorized information or possibly conduct further attacks. The highest threat from this vulnerability is to data confidentiality and integrity.	7.4	More Details
CVE-2020-26233	Git Credential Manager Core (GCM Core) is a secure Git credential helper built on .NET Core that runs on Windows and macOS. In Git Credential Manager Core before version 2.0.289, when recursively cloning a Git repository on Windows with submodules, Git will first clone the top-level repository and then recursively clone all submodules by starting new Git processes from the top-level working directory. If a malicious git.exe executable is present in the top-level repository then this binary will be started by Git Credential Manager Core when attempting to read configuration, and not git.exe as found on the %PATH%. This only affects GCM Core on Windows, not macOS or Linux-based distributions. GCM Core version 2.0.289 contains the fix for this vulnerability, and is available from the project's GitHub releases page. GCM Core 2.0.289 is also bundled in the latest Git for Windows release; version 2.29.2(3). As a workaround, users should avoid recursively cloning untrusted repositories with the --recurse-submodules option.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28939	OpenClinic version 0.8.2 is affected by a medical/test_new.php insecure file upload vulnerability. This vulnerability allows authenticated users (with substantial privileges) to upload malicious files, such as PHP web shells, which can lead to arbitrary code execution on the application server.	7.2	More Details
CVE-2020-26122	Inspur NF5266M5 through 3.21.2 and other server M5 devices allow remote code execution via administrator privileges. The Baseboard Management Controller (BMC) program of INSPUR server is weak in checking the firmware and lacks the signature verification mechanism, the attacker who obtains the administrator's rights can control the BMC by inserting malicious code into the firmware program and bypassing the current verification mechanism to upgrade the BMC.	7.2	More Details
CVE-2020-27752	A flaw was found in ImageMagick in MagickCore/quantum-private.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger a heap buffer overflow. This would most likely lead to an impact to application availability, but could potentially lead to an impact to data integrity as well. This flaw affects ImageMagick versions prior to 7.0.9-0.	7.1	More Details
CVE-2020-26255	Kirby is a CMS. In Kirby CMS (getkirby/cms) before version 3.4.5, and Kirby Panel before version 2.5.14 , an editor with full access to the Kirby Panel can upload a PHP .phar file and execute it on the server. This vulnerability is critical if you might have potential attackers in your group of authenticated Panel users, as they can gain access to the server with such a Phar file. Visitors without Panel access *cannot* use this attack vector. The problem has been patched in Kirby 2.5.14 and Kirby 3.4.5. Please update to one of these or a later version to fix the vulnerability. Note: Kirby 2 reaches end of life on December 31, 2020. We therefore recommend to upgrade your Kirby 2 sites to Kirby 3. If you cannot upgrade, we still recommend to update to Kirby 2.5.14.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26253	Kirby is a CMS. In Kirby CMS (getkirby/cms) before version 3.3.6, and Kirby Panel before version 2.5.14 there is a vulnerability in which the admin panel may be accessed if hosted on a .dev domain. In order to protect new installations on public servers that don't have an admin account for the Panel yet, we block account registration there by default. This is a security feature, which we implemented years ago in Kirby 2. It helps to avoid that you forget registering your first admin account on a public server. In this case – without our security block – someone else might theoretically be able to find your site, find out it's running on Kirby, find the Panel and then register the account first. It's an unlikely situation, but it's still a certain risk. To be able to register the first Panel account on a public server, you have to enforce the installer via a config setting. This helps to push all users to the best practice of registering your first Panel account on your local machine and upload it together with the rest of the site. This installation block implementation in Kirby versions before 3.3.6 still assumed that .dev domains are local domains, which is no longer true. In the meantime, those domains became publicly available. This means that our installation block is no longer working as expected if you use a .dev domain for your Kirby site. Additionally the local installation check may also fail if your site is behind a reverse proxy. You are only affected if you use a .dev domain or your site is behind a reverse proxy and you have not yet registered your first Panel account on the public server and someone finds your site and tries to login at `yourdomain.dev/panel` before you register your first account. You are not affected if you have already created one or multiple Panel accounts (no matter if on a .dev domain or behind a reverse proxy). The problem has been patched in Kirby 3.3.6. Please upgrade to this or a later version to fix the vulnerability.	6.8	More Details
CVE-2012-0955	software-properties was vulnerable to a person-in-the-middle attack due to incorrect TLS certificate validation in softwareproperties/ppa.py. software-properties didn't check TLS certificates under python2 and only checked certificates under python3 if a valid certificate bundle was provided. Fixed in software-properties version 0.92.	6.8	More Details
CVE-2020-27348	In some conditions, a snap package built by snapcraft includes the current directory in LD_LIBRARY_PATH, allowing a malicious snap to gain code execution within the context of another snap if both plug the home interface or similar. This issue affects snapcraft versions prior to 4.4.4, prior to 2.43.1+16.04.1, and prior to 2.43.1+18.04.1.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26244	Python oic is a Python OpenID Connect implementation. In Python oic before version 1.2.1, there are several related cryptographic issues affecting client implementations that use the library. The issues are: 1) The IdToken signature algorithm was not checked automatically, but only if the expected algorithm was passed in as a kwarg. 2) JWA `none` algorithm was allowed in all flows. 3) oic.consumer.Consumer.parse_authz returns an unverified IdToken. The verification of the token was left to the discretion of the implementator. 4) iat claim was not checked for sanity (i.e. it could be in the future). These issues are patched in version 1.2.1.	6.8	More Details
CVE-2020-26248	In the PrestaShop module "productcomments" before version 4.2.1, an attacker can use a Blind SQL injection to retrieve data or stop the MySQL service. The problem is fixed in 4.2.1 of the module.	6.8	More Details
CVE-2020-4102	HCL Notes is susceptible to a Buffer Overflow vulnerability in DXL due to improper validation of user input. A successful exploit could enable an attacker to crash Notes or execute attacker-controlled code on the client system.	6.7	More Details
CVE-2020-13496	An exploitable vulnerability exists in the way Pixar OpenUSD 20.05 handles parses certain encoded types. A specially crafted malformed file can trigger an arbitrary out of bounds memory access in TfToken Type Index. This vulnerability could be used to bypass mitigations and aid further exploitation. To trigger this vulnerability, the victim needs to access an attacker-provided malformed file.	6.5	More Details
CVE-2020-25711	A flaw was found in infinispan 10 REST API, where authorization permissions are not checked while performing some server management operations. When authz is enabled, any user with authentication can perform operations like shutting down the server without the ADMIN role.	6.5	More Details
CVE-2020-28206	An issue was discovered in Bitrix24 Bitrix Framework (1c site management) 20.0. An "User enumeration and Improper Restriction of Excessive Authentication Attempts" vulnerability exists in the admin login form, allowing a remote user to enumerate users in the administrator group. This also allows brute-force attacks on the passwords of users not in the administrator group.	6.5	More Details
CVE-2020-9849	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0, iTunes for Windows 12.10.9, iCloud for Windows 11.5, tvOS 14.0. A remote attacker may be able to leak memory.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21270	Versions less than 0.0.6 of the Node.js stringstream module are vulnerable to an out-of-bounds read because of allocation of uninitialized buffers when a number is passed in the input stream (when using Node.js 4.x).	6.5	More Details
CVE-2020-25265	AppImage libappimage before 1.0.3 allows attackers to trigger an overwrite of a system-installed .desktop file by providing a .desktop file that contains Name= with path components.	6.5	More Details
CVE-2020-13945	In Apache APISIX, the user enabled the Admin API and deleted the Admin API access IP restriction rules. Eventually, the default token is allowed to access APISIX management data. This affects versions 1.2, 1.3, 1.4, 1.5.	6.5	More Details
CVE-2020-9922	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra. Processing a maliciously crafted email may lead to writing arbitrary files.	6.5	More Details
CVE-2020-14383	A flaw was found in samba's DNS server. An authenticated user could use this flaw to the RPC server to crash. This RPC server, which also serves protocols other than dnsserver, will be restarted after a short delay, but it is easy for an authenticated non administrative attacker to crash it again as soon as it returns. The Samba DNS server itself will continue to operate, but many RPC services will not.	6.5	More Details
CVE-2020-10014	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Big Sur 11.0.1. A malicious application may be able to break out of its sandbox.	6.3	More Details
CVE-2020-14369	This release fixes a Cross Site Request Forgery vulnerability was found in Red Hat CloudForms which forces end users to execute unwanted actions on a web application in which the user is currently authenticated. An attacker can make a forgery HTTP request to the server by crafting custom flash file which can force the user to perform state changing requests like provisioning VMs, running ansible playbooks and so forth.	6.3	More Details
CVE-2020-29572	app/View/Elements/genericElements/SingleViews/Fields/genericField.ctp in MISP 2.4.135 has XSS via the authkey comment field.	6.1	More Details
CVE-2020-29239	Online Birth Certificate System Project V 1.0 is affected by cross-site scripting (XSS). This vulnerability can result in an attacker injecting the XSS payload in the User Registration section. When an admin visits the View Detail of Application section from the admin panel, the attacker can able to steal the cookie according to the crafted payload.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14206	The DiveBook plugin 1.1.4 for WordPress is prone to unauthenticated XSS within the filter function (via an arbitrary parameter).	6.1	More Details
CVE-2020-5679	Improper restriction of rendered UI layers or frames in EC-CUBE versions from 3.0.0 to 3.0.18 leads to clickjacking attacks. If a user accesses a specially crafted page while logged into the administrative page, unintended operations may be conducted.	6.1	More Details
CVE-2020-5678	Stored cross-site scripting vulnerability in GROWI v3.8.1 and earlier allows remote attackers to inject arbitrary script via unspecified vectors.	6.1	More Details
CVE-2020-10012	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Big Sur 11.0.1. Processing a maliciously crafted document may lead to a cross site scripting attack.	6.1	More Details
CVE-2020-5677	Reflected cross-site scripting vulnerability in GROWI v4.0.0 and earlier allows remote attackers to inject arbitrary script via unspecified vectors.	6.1	More Details
CVE-2020-5638	Cross-site scripting vulnerability in desknet's NEO (desknet's NEO Small License V5.5 R1.5 and earlier, and desknet's NEO Enterprise License V5.5 R1.5 and earlier) allows remote attackers to inject arbitrary script via unspecified vectors.	6.1	More Details
CVE-2020-27783	A XSS vulnerability was discovered in python-lxml's clean module. The module's parser didn't properly imitate browsers, which caused different behaviors between the sanitizer and the user's page. A remote attacker could exploit this flaw to run arbitrary HTML/JS code.	6.1	More Details
CVE-2020-25664	In WriteOnePNGImage() of the PNG coder at coders/png.c, an improper call to AcquireVirtualMemory() and memset() allows for an out-of-bounds write later when PopShortPixel() from MagickCore/quantum-private.h is called. The patch fixes the calls by adding 256 to rowbytes. An attacker who is able to supply a specially crafted image could affect availability with a low impact to data integrity. This flaw affects ImageMagick versions prior to 6.9.10-68 and 7.0.8-68.	6.1	More Details
CVE-2020-25631	A vulnerability was found in Moodle 3.9 to 3.9.1, 3.8 to 3.8.4 and 3.7 to 3.7.7 where it was possible to include JavaScript in a book's chapter title, which was not escaped on the "Add new chapter" page. This is fixed in 3.9.2, 3.8.5 and 3.7.8.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25628	The filter in the tag manager required extra sanitizing to prevent a reflected XSS risk. This affects 3.9 to 3.9.1, 3.8 to 3.8.4, 3.7 to 3.7.7, 3.5 to 3.5.13 and earlier unsupported versions. Fixed in 3.9.2, 3.8.5, 3.7.8 and 3.5.14.	6.1	More Details
CVE-2020-27409	OpenSIS Community Edition before 7.5 is affected by a cross-site scripting (XSS) vulnerability in SideForStudent.php via the modname parameter.	6.1	More Details
CVE-2020-28727	Cross-site scripting (XSS) exists in SeedDMS 6.0.13 via the folderid parameter to views/bootstrap/class.DropFolderChooser.php.	6.1	More Details
CVE-2020-27816	The elasticsearch-operator does not validate the namespace where kibana logging resource is created and due to that it is possible to replace the original openshift-logging console link (kibana console) to different one, created based on the new CR for the new kibana resource. This could lead to an arbitrary URL redirection or the openshift-logging console link damage. This flaw affects elasticsearch-operator-container versions before 4.7.	6.1	More Details
CVE-2020-29565	An issue was discovered in OpenStack Horizon before 15.3.2, 16.x before 16.2.1, 17.x and 18.x before 18.3.3, 18.4.x, and 18.5.x. There is a lack of validation of the "next" parameter, which would allow someone to supply a malicious URL in Horizon that can cause an automatic redirect to the provided malicious URL.	6.1	More Details
CVE-2020-29456	Multiple cross-site scripting (XSS) vulnerabilities in Papermerge before 1.5.2 allow remote attackers to inject arbitrary web script or HTML via the rename, tag, upload, or create folder function. The payload can be in a folder, a tag, or a document's filename. If email consumption is configured in Papermerge, a malicious document can be sent by email and is automatically uploaded into the Papermerge web application. Therefore, no authentication is required to exploit XSS if email consumption is configured. Otherwise authentication is required.	6.1	More Details
CVE-2020-27821	A flaw was found in the memory management API of QEMU during the initialization of a memory region cache. This issue could lead to an out-of-bounds write access to the MSI-X table while performing MMIO operations. A guest user may abuse this flaw to crash the QEMU process on the host, resulting in a denial of service. This flaw affects QEMU versions prior to 5.2.0.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1971	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).	5.9	More Details
CVE-2020-27822	A flaw was found in Wildfly affecting versions 19.0.0.Final, 19.1.0.Final, 20.0.0.Final, 20.0.1.Final, and 21.0.0.Final. When an application uses the OpenTracing API's java-interceptors, there is a possibility of a memory leak. This flaw allows an attacker to impact the availability of the server. The highest threat from this vulnerability is to system availability.	5.9	More Details
CVE-2020-26256	Fast-csv is an npm package for parsing and formatting CSVs or any other delimited value file in node. In fast-cvs before version 4.3.6 there is a possible ReDoS vulnerability (Regular Expression Denial of Service) when using ignoreEmpty option when parsing. This has been patched in `v4.3.6` You will only be affected by this if you use the `ignoreEmpty` parsing option. If you do use this option it is recommended that you upgrade to the latest version `v4.3.6` This vulnerability was found using a CodeQL query which identified `EMPTY_ROW_REGEXP` regular expression as vulnerable.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13494	A heap overflow vulnerability exists in the Pixar OpenUSD 20.05 parsing of compressed string tokens in binary USD files. A specially crafted malformed file can trigger a heap overflow which can result in out of bounds memory access which could lead to information disclosure. This vulnerability could be used to bypass mitigations and aid further exploitation. To trigger this vulnerability, victim needs to access an attacker-provided malformed file.	5.5	More Details
CVE-2020-25676	In CatromWeights(), MeshInterpolate(), InterpolatePixelChannel(), InterpolatePixelChannels(), and InterpolatePixelInfo(), which are all functions in /MagickCore/pixel.c, there were multiple unconstrained pixel offset calculations which were being used with the floor() function. These calculations produced undefined behavior in the form of out-of-range and integer overflows, as identified by UndefinedBehaviorSanitizer. These instances of undefined behavior could be triggered by an attacker who is able to supply a crafted input file to be processed by ImageMagick. These issues could impact application availability or potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0.	5.5	More Details
CVE-2020-9977	A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A malicious application may be able to determine a user's open tabs in Safari.	5.5	More Details
CVE-2020-9974	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, tvOS 14.2, watchOS 7.1. A malicious application may be able to determine kernel memory layout.	5.5	More Details
CVE-2020-27929	A logic issue existed in the handling of Group FaceTime calls. The issue was addressed with improved state management. This issue is fixed in iOS 12.4.9. A user may send video in Group FaceTime calls without knowing that they have done so.	5.5	More Details
CVE-2020-9969	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. A local user may be able to view senstive user information.	5.5	More Details
CVE-2020-9988	The issue was addressed with improved deletion. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A local user may be able to discover a user’s deleted messages.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27950	A memory initialization issue was addressed. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. A malicious application may be able to disclose kernel memory.	5.5	More Details
CVE-2020-9963	The issue was addressed with improved handling of icon caches. This issue is fixed in macOS Big Sur 11.0.1, iOS 14.0 and iPadOS 14.0. A malicious app may be able to determine the existence of files on the computer.	5.5	More Details
CVE-2020-9944	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. An application may be able to read restricted memory.	5.5	More Details
CVE-2020-27925	An issue existed in the handling of incoming calls. The issue was addressed with additional state checks. This issue is fixed in iOS 14.2 and iPadOS 14.2. A user may answer two calls simultaneously without indication they have answered a second call.	5.5	More Details
CVE-2020-9989	The issue was addressed with improved deletion. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, iOS 14.0 and iPadOS 14.0. A local user may be able to discover a user's deleted messages.	5.5	More Details
CVE-2020-27750	A flaw was found in ImageMagick in MagickCore/colorspace-private.h and MagickCore/quantum.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned char` and math division by zero. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.8-68.	5.5	More Details
CVE-2020-25266	AppImage appimaged before 1.0.3 does not properly check whether a downloaded file is a valid appimage. For example, it will accept a crafted mp3 file that contains an appimage, and install it.	5.5	More Details
CVE-2020-27896	A path handling issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.0.1. A remote attacker may be able to modify the file system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13498	An exploitable vulnerability exists in the way Pixar OpenUSD 20.05 handles parses certain encoded types. A specially crafted malformed file can trigger an arbitrary out of bounds memory access which could lead to information disclosure. This vulnerability could be used to bypass mitigations and aid further exploitation. To trigger this vulnerability, the victim needs to access an attacker-provided malformed file.	5.5	More Details
CVE-2020-25663	A call to ConformPixelInfo() in the SetImageAlphaChannel() routine of /MagickCore/channel.c caused a subsequent heap-use-after-free or heap-buffer-overflow READ when GetPixelRed() or GetPixelBlue() was called. This could occur if an attacker is able to submit a malicious image file to be processed by ImageMagick and could lead to denial of service. It likely would not lead to anything further because the memory is used as pixel data and not e.g. a function pointer. This flaw affects ImageMagick versions prior to 7.0.9-0.	5.5	More Details
CVE-2020-25665	The PALM image coder at coders/palm.c makes an improper call to AcquireQuantumMemory() in routine WritePALMImage() because it needs to be offset by 256. This can cause a out-of-bounds read later on in the routine. The patch adds 256 to bytes_per_row in the call to AcquireQuantumMemory(). This could cause impact to reliability. This flaw affects ImageMagick versions prior to 7.0.8-68.	5.5	More Details
CVE-2020-25674	WriteOnePNGImage() from coders/png.c (the PNG coder) has a for loop with an improper exit condition that can allow an out-of-bounds READ via heap-buffer-overflow. This occurs because it is possible for the colormap to have less than 256 valid values but the loop condition will loop 256 times, attempting to pass invalid colormap data to the event logger. The patch replaces the hardcoded 256 value with a call to MagickMin() to ensure the proper value is used. This could impact application availability when a specially crafted input file is processed by ImageMagick. This flaw affects ImageMagick versions prior to 7.0.8-68.	5.5	More Details
CVE-2020-27898	A denial of service issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.0.1. An attacker may be able to bypass Managed Frame Protection.	5.5	More Details
CVE-2020-27900	An issue existed in the handling of snapshots. The issue was resolved with improved permissions logic. This issue is fixed in macOS Big Sur 11.0.1. A malicious application may be able to preview files it does not have access to.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13497	An exploitable vulnerability exists in the way Pixar OpenUSD 20.05 handles parses certain encoded types. A specially crafted malformed file can trigger an arbitrary out of bounds memory access in String Type Index. This vulnerability could be used to bypass mitigations and aid further exploitation. To trigger this vulnerability, the victim needs to access an attacker-provided malformed file.	5.5	More Details
CVE-2020-25704	A flaw memory leak in the Linux kernel performance monitoring subsystem was found in the way if using PERF_EVENT_IOC_SET_FILTER. A local user could use this flaw to starve the resources causing denial of service.	5.5	More Details
CVE-2020-27756	In ParseMetaGeometry() of MagickCore/geometry.c, image height and width calculations can lead to divide-by-zero conditions which also lead to undefined behavior. This flaw can be triggered by a crafted input file processed by ImageMagick and could impact application availability. The patch uses multiplication in addition to the function `PerceptibleReciprocal()` in order to prevent such divide-by-zero conditions. This flaw affects ImageMagick versions prior to 7.0.9-0.	5.5	More Details
CVE-2020-27753	There are several memory leaks in the MIFF coder in /coders/miff.c due to improper image depth values, which can be triggered by a specially crafted input file. These leaks could potentially lead to an impact to application availability or cause a denial of service. It was originally reported that the issues were in `AcquireMagickMemory()` because that is where LeakSanitizer detected the leaks, but the patch resolves issues in the MIFF coder, which incorrectly handles data being passed to `AcquireMagickMemory()`. This flaw affects ImageMagick versions prior to 7.0.9-0.	5.5	More Details
CVE-2020-25667	TIFFGetProfiles() in /coders/tiff.c calls strstr() which causes a large out-of-bounds read when it searches for `"dc:format=\"image/dng\"` within `profile` due to improper string handling, when a crafted input file is provided to ImageMagick. The patch uses a StringInfo type instead of a raw C string to remedy this. This could cause an impact to availability of the application. This flaw affects ImageMagick versions prior to 7.0.9-0.	5.5	More Details
CVE-2020-9943	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0. A malicious application may be able to read restricted memory.	5.5	More Details
CVE-2020-23741	In AnyView (network police) network monitoring software 4.6.0.1, there is a local denial of service vulnerability in AnyView, attackers can use a constructed program to cause a computer crash (BSOD).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29561	An issue was discovered in SonicBOOM riscv-boom 3.0.0. For LR, it does not avoid acquiring a reservation in the case where a load translates successfully but still generates an exception.	5.5	More Details
CVE-2020-23736	There is a local denial of service vulnerability in DaDa accelerator 5.6.19.816,, attackers can use constructed programs to cause computer crashes (BSOD).	5.5	More Details
CVE-2020-23727	There is a local denial of service vulnerability in the Antiy Zhijia Terminal Defense System 5.0.2.10121559 and an attacker can cause a computer crash (BSOD).	5.5	More Details
CVE-2020-23726	There is a local denial of service vulnerability in Wise Care 365 5.5.4, attackers can cause computer crash (BSOD).	5.5	More Details
CVE-2020-13524	An out-of-bounds memory corruption vulnerability exists in the way Pixar OpenUSD 20.05 uses SPECS data from binary USD files. A specially crafted malformed file can trigger an out-of-bounds memory access and modification which results in memory corruption. To trigger this vulnerability, the victim needs to access an attacker-provided malformed file.	5.5	More Details
CVE-2020-10002	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 14.2 and iPadOS 14.2, iCloud for Windows 11.5, tvOS 14.2, iTunes 12.11 for Windows. A local user may be able to read arbitrary files.	5.5	More Details
CVE-2020-28935	NLnet Labs Unbound, up to and including version 1.12.0, and NLnet Labs NSD, up to and including version 4.3.3, contain a local vulnerability that would allow for a local symlink attack. When writing the PID file, Unbound and NSD create the file if it is not there, or open an existing file for writing. In case the file was already present, they would follow symlinks if the file happened to be a symlink instead of a regular file. An additional chown of the file would then take place after it was written, making the user Unbound/NSD is supposed to run as the new owner of the file. If an attacker has local access to the user Unbound/NSD runs as, she could create a symlink in place of the PID file pointing to a file that she would like to erase. If then Unbound/NSD is killed and the PID file is not cleared, upon restarting with root privileges, Unbound/NSD will rewrite any file pointed at by the symlink. This is a local vulnerability that could create a Denial of Service of the system Unbound/NSD is running on. It requires an attacker having access to the limited permission user Unbound/NSD runs as and point through the symlink to a critical file on the system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10006	This issue was addressed with improved entitlements. This issue is fixed in macOS Big Sur 11.0.1. A malicious application may be able to access restricted files.	5.5	More Details
CVE-2020-17521	Apache Groovy provides extension methods to aid with creating temporary directories. Prior to this fix, Groovy's implementation of those extension methods was using a now superseded Java JDK method call that is potentially not secure on some operating systems in some contexts. Users not using the extension methods mentioned in the advisory are not affected, but may wish to read the advisory for further details. Versions Affected: 2.0 to 2.4.20, 2.5.0 to 2.5.13, 3.0.0 to 3.0.6, and 4.0.0-alpha-1. Fixed in versions 2.4.21, 2.5.14, 3.0.7, 4.0.0-alpha-2.	5.5	More Details
CVE-2020-10007	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1. A malicious application may be able to determine kernel memory layout.	5.5	More Details
CVE-2020-23738	There is a local denial of service vulnerability in Advanced SystemCare 13 PRO 13.5.0.174. Attackers can use a constructed program to cause a computer crash (BSOD)	5.5	More Details
CVE-2020-26513	An issue was discovered in Intland codeBeamer ALM 10.x through 10.1.SP4. The ReqIF XML data, used by the codebeamer ALM application to import projects, is parsed by insecurely configured software components, which can be abused for XML External Entity Attacks.	5.5	More Details
CVE-2020-10009	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1. A sandboxed process may be able to circumvent sandbox restrictions.	5.5	More Details
CVE-2020-27762	A flaw was found in ImageMagick in coders/hdr.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned char`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to ImageMagick 7.0.8-68.	5.5	More Details
CVE-2020-28916	hw/net/e1000e_core.c in QEMU 5.0.0 has an infinite loop via an RX descriptor with a NULL buffer address.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27760	In `GammaImage()` of /MagickCore/enhance.c, depending on the `gamma` value, it's possible to trigger a divide-by-zero condition when a crafted input file is processed by ImageMagick. This could lead to an impact to application availability. The patch uses the `PerceptibleReciprocal()` to prevent the divide-by-zero from occurring. This flaw affects ImageMagick versions prior to ImageMagick 7.0.8-68.	5.5	More Details
CVE-2020-27894	The issue was addressed with additional user controls. This issue is fixed in macOS Big Sur 11.0.1. Users may be unable to remove metadata indicating where files were downloaded from.	5.5	More Details
CVE-2020-27770	Due to a missing check for 0 value of `replace_extent`, it is possible for offset `p` to overflow in SubstituteString(), causing potential impact to application availability. This could be triggered by a crafted input file that is processed by ImageMagick. This flaw affects ImageMagick versions prior to 7.0.8-68.	5.5	More Details
CVE-2020-25677	A flaw was found in Ceph-ansible v4.0.41 where it creates an /etc/ceph/iscsi-gateway.conf with insecure default permissions. This flaw allows any user on the system to read sensitive information within this file. The highest threat from this vulnerability is to confidentiality.	5.5	More Details
CVE-2020-28938	OpenClinic version 0.8.2 is affected by a stored XSS vulnerability in lib/Check.php that allows users of the application to force actions on behalf of other users.	5.4	More Details
CVE-2020-25955	SourceCodester Student Management System Project in PHP version 1.0 is vulnerable to stored a cross-site scripting (XSS) via the 'add subject' tab.	5.4	More Details
CVE-2020-29539	A Cross-Site Scripting (XSS) issue in WebUI Translation in Systran Pure Neural Server before 9.7.0 allows a threat actor to have a remote authenticated user run JavaScript from a malicious site.	5.4	More Details
CVE-2020-14205	The DiveBook plugin 1.1.4 for WordPress is prone to improper access control in the Log Dive form because it fails to perform authorization checks. An attacker may leverage this issue to manipulate the integrity of dive logs.	5.3	More Details
CVE-2020-14207	The DiveBook plugin 1.1.4 for WordPress was prone to a SQL injection within divelog.php, allowing unauthenticated users to retrieve data from the database via the divelog.php filter_diver parameter.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13956	Apache HttpClient versions prior to version 4.5.13 and 5.0.3 can misinterpret malformed authority component in request URIs passed to the library as java.net.URI object and pick the wrong target host for request execution.	5.3	More Details
CVE-2020-2323	Jenkins Chaos Monkey Plugin 0.4 and earlier does not perform permission checks in an HTTP endpoint, allowing attackers with Overall/Read permission to access the Chaos Monkey page and to see the history of actions.	5.3	More Details
CVE-2020-29562	The iconv function in the GNU C Library (aka glibc or libc6) 2.30 to 2.32, when converting UCS4 text containing an irreversible character, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.	4.8	More Details
CVE-2020-25449	Cross Site Scripting (XSS) vulnerability in Arachnys Cabot 0.11.12 can be exploited via the Address column.	4.8	More Details
CVE-2020-29240	Lepton-CMS 4.7.0 is affected by cross-site scripting (XSS). An attacker can inject the XSS payload in the URL field of the admin page and each time an admin visits the Menu-Pages-Pages Overview section, the XSS will be triggered.	4.8	More Details
CVE-2020-26234	Opencast before versions 8.9 and 7.9 disables HTTPS hostname verification of its HTTP client used for a large portion of Opencast's HTTP requests. Hostname verification is an important part when using HTTPS to ensure that the presented certificate is valid for the host. Disabling it can allow for man-in-the-middle attacks. This problem is fixed in Opencast 7.9 and Opencast 8.8 Please be aware that fixing the problem means that Opencast will not simply accept any self-signed certificates any longer without properly importing them. If you need those, please make sure to import them into the Java key store. Better yet, get a valid certificate.	4.8	More Details
CVE-2020-8566	In Kubernetes clusters using Ceph RBD as a storage provisioner, with logging level of at least 4, Ceph RBD admin secrets can be written to logs. This occurs in kube-controller-manager's logs during provisioning of Ceph RBD persistent claims. This affects < v1.19.3, < v1.18.10, < v1.17.13.	4.7	More Details
CVE-2020-8565	In Kubernetes, if the logging level is set to at least 9, authorization and bearer tokens will be written to log files. This can occur both in API server logs and client tool output like kubectl. This affects <= v1.19.3, <= v1.18.10, <= v1.17.13, < v1.20.0-alpha2.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8564	In Kubernetes clusters using a logging level of at least 4, processing a malformed docker config file will result in the contents of the docker config file being leaked, which can include pull secrets or other registry credentials. This affects < v1.19.3, < v1.18.10, < v1.17.13.	4.7	More Details
CVE-2020-8563	In Kubernetes clusters using VSphere as a cloud provider, with a logging level set to 4 or above, VSphere cloud credentials will be leaked in the cloud controller manager's log. This affects < v1.19.3.	4.7	More Details
CVE-2020-27902	An authentication issue was addressed with improved state management. This issue is fixed in iOS 14.2 and iPadOS 14.2. A person with physical access to an iOS device may be able to access stored passwords without authentication.	4.6	More Details
CVE-2020-16123	An Ubuntu-specific patch in PulseAudio created a race condition where the snap policy module would fail to identify a client connection from a snap as coming from a snap if SCM_CREDENTIALS were missing, allowing the snap to connect to PulseAudio without proper confinement. This could be exploited by an attacker to expose sensitive information. Fixed in 1:13.99.3-1ubuntu2, 1:13.99.2-1ubuntu2.1, 1:13.99.1-1ubuntu3.8, 1:11.1-1ubuntu7.11, and 1:8.0-0ubuntu3.15.	4.4	More Details
CVE-2020-9987	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in Safari 14.0. Visiting a malicious website may lead to address bar spoofing.	4.3	More Details
CVE-2020-9945	A spoofing issue existed in the handling of URLs. This issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, Safari 14.0.1. Visiting a malicious website may lead to address bar spoofing.	4.3	More Details
CVE-2020-9942	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1, Safari 13.1.2. Visiting a malicious website may lead to address bar spoofing.	4.3	More Details
CVE-2020-9993	The issue was addressed with improved UI handling. This issue is fixed in watchOS 7.0, Safari 14.0, iOS 14.0 and iPadOS 14.0. Visiting a malicious website may lead to address bar spoofing.	4.3	More Details
CVE-2020-14318	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29454	Editors/LogViewerController.cs in Umbraco through 8.9.1 allows a user to visit a logviewer endpoint even if they lack Applications.Settings access.	4.3	More Details
CVE-2020-25656	A flaw was found in the Linux kernel. A use-after-free was found in the way the console subsystem was using ioctls KDGKBSENT and KDSKBSENT. A local user could use this flaw to get read memory access out of bounds. The highest threat from this vulnerability is to data confidentiality.	4.1	More Details
CVE-2020-27774	A flaw was found in ImageMagick in MagickCore/statistic.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of a too large shift for 64-bit type `ssize_t`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0.	3.3	More Details
CVE-2020-27754	In IntensityCompare() of /magick/quantize.c, there are calls to PixelPacketIntensity() which could return overflowed values to the caller when ImageMagick processes a crafted input file. To mitigate this, the patch introduces and uses the ConstrainPixelIntensity() function, which forces the pixel intensities to be within the proper bounds in the event of an overflow. This flaw affects ImageMagick versions prior to 6.9.10-69 and 7.0.8-69.	3.3	More Details
CVE-2020-27755	in SetImageExtent() of /MagickCore/image.c, an incorrect image depth size can cause a memory leak because the code which checks for the proper image depth size does not reset the size in the event there is an invalid size. The patch resets the depth to a proper size before throwing an exception. The memory leak can be triggered by a crafted input file that is processed by ImageMagick and could cause an impact to application reliability, such as denial of service. This flaw affects ImageMagick versions prior to 7.0.9-0.	3.3	More Details
CVE-2020-27818	A flaw was found in the check_chunk_name() function of pngcheck-2.4.0. An attacker able to pass a malicious file to be processed by pngcheck could cause a temporary denial of service, posing a low risk to application availability.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27757	A floating point math calculation in ScaleAnyToQuantum() of /MagickCore/quantum-private.h could lead to undefined behavior in the form of a value outside the range of type unsigned long long. The flaw could be triggered by a crafted input file under certain conditions when it is processed by ImageMagick. Red Hat Product Security marked this as Low because although it could potentially lead to an impact to application availability, no specific impact was shown in this case. This flaw affects ImageMagick versions prior to 7.0.8-68.	3.3	More Details
CVE-2020-27758	A flaw was found in ImageMagick in coders/txt.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned long long`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.8-68.	3.3	More Details
CVE-2020-27751	A flaw was found in ImageMagick in MagickCore/quantum-export.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned long long` as well as a shift exponent that is too large for 64-bit type. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0.	3.3	More Details
CVE-2020-27765	A flaw was found in ImageMagick in MagickCore/segment.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0.	3.3	More Details
CVE-2020-27767	A flaw was found in ImageMagick in MagickCore/quantum.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of types `float` and `unsigned char`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27771	In RestoreMSCWarning() of /coders/pdf.c there are several areas where calls to GetPixelIndex() could result in values outside the range of representable for the unsigned char type. The patch casts the return value of GetPixelIndex() to ssize_t type to avoid this bug. This undefined behavior could be triggered when ImageMagick processes a crafted pdf file. Red Hat Product Security marked this as Low severity because although it could potentially lead to an impact to application availability, no specific impact was demonstrated in this case. This flaw affects ImageMagick versions prior to 7.0.9-0.	3.3	More Details
CVE-2020-27775	A flaw was found in ImageMagick in MagickCore/quantum.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type unsigned char. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0.	3.3	More Details
CVE-2020-27761	WritePALMImage() in /coders/palm.c used size_t casts in several areas of a calculation which could lead to values outside the range of representable type `unsigned long` undefined behavior when a crafted input file was processed by ImageMagick. The patch casts to `ssize_t` instead to avoid this issue. Red Hat Product Security marked the Severity as Low because although it could potentially lead to an impact to application availability, no specific impact was shown in this case. This flaw affects ImageMagick versions prior to ImageMagick 7.0.9-0.	3.3	More Details
CVE-2020-27776	A flaw was found in ImageMagick in MagickCore/statistic.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type unsigned long. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0.	3.3	More Details
CVE-2020-27772	A flaw was found in ImageMagick in coders/bmp.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned int`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27773	A flaw was found in ImageMagick in MagickCore/gem-private.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned char` or division by zero. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.9-0.	3.3	More Details
CVE-2020-25675	In the CropImage() and CropImageToTiles() routines of MagickCore/transform.c, rounding calculations performed on unconstrained pixel offsets was causing undefined behavior in the form of integer overflow and out-of-range values as reported by UndefinedBehaviorSanitizer. Such issues could cause a negative impact to application availability or other problems related to undefined behavior, in cases where ImageMagick processes untrusted input data. The upstream patch introduces functionality to constrain the pixel offsets and prevent these issues. This flaw affects ImageMagick versions prior to 7.0.9-0.	3.3	More Details
CVE-2020-27763	A flaw was found in ImageMagick in MagickCore/resize.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.8-68.	3.3	More Details
CVE-2020-27764	In /MagickCore/statistic.c, there are several areas in ApplyEvaluateOperator() where a size_t cast should have been a ssize_t cast, which causes out-of-range values under some circumstances when a crafted input file is processed by ImageMagick. Red Hat Product Security marked this as Low severity because although it could potentially lead to an impact to application availability, no specific impact was shown in this case. This flaw affects ImageMagick versions prior to 6.9.10-69.	3.3	More Details
CVE-2020-25666	There are 4 places in HistogramCompare() in MagickCore/histogram.c where an integer overflow is possible during simple math calculations. This occurs in the rgb values and `count` value for a color. The patch uses casts to `ssize_t` type for these calculations, instead of `int`. This flaw could impact application reliability in the event that ImageMagick processes a crafted input file. This flaw affects ImageMagick versions prior to 7.0.9-0.	3.3	More Details
CVE-2020-27895	An information disclosure issue existed in the transition of program state. This issue was addressed with improved state handling. This issue is fixed in iTunes 12.11 for Windows. A malicious application may be able to access local users Apple IDs.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27759	In IntensityCompare() of /MagickCore/quantize.c, a double value was being casted to int and returned, which in some cases caused a value outside the range of type `int` to be returned. The flaw could be triggered by a crafted input file under certain conditions when processed by ImageMagick. Red Hat Product Security marked this as Low severity because although it could potentially lead to an impact to application availability, no specific impact was shown in this case. This flaw affects ImageMagick versions prior to 7.0.8-68.	3.3	More Details
CVE-2020-25723	A reachable assertion issue was found in the USB EHCI emulation code of QEMU. It could occur while processing USB requests due to missing handling of DMA memory map failure. A malicious privileged user within the guest may abuse this flaw to send bogus USB requests and crash the QEMU process on the host, resulting in a denial of service.	3.2	More Details
CVE-2020-28923	An issue was discovered in Play Framework 2.8.0 through 2.8.4. Carefully crafted JSON payloads sent as a form field lead to Data Amplification. This affects users migrating from a Play version prior to 2.8.0 that used the Play Java API to serialize classes with protected or private fields to JSON.	2.7	More Details
CVE-2020-27641	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-29136. Reason: This candidate is a reservation duplicate of CVE-2020-29136. Notes: All CVE users should reference CVE-2020-29136 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details