

S920X00
iBMC V631

版本说明书

文档版本	01
发布日期	2021-09-04

版权所有 ©北京神州数码云科信息技术有限公司 2021。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



和其他北京神州数码云科信息技术有限公司商标均为北京神州数码云科信息技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受北京神州数码云科信息技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，北京神州数码云科信息技术有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

北京神州数码云科信息技术有限公司

地址：北京市海淀区上地九街 9 号数码科技广场

网址：www.shenzhoukuntai.com

客户服务邮箱：kuntai_support@digitalchina.com

客户服务电话：400-810-9119

目 录

1 V631 版本说明书.....1

2 V626 版本说明书.....2

3 V625 版本说明书.....3

4 V622 版本说明书.....4

5 V620 版本说明书.....6

6 V616 版本说明书.....7

7 V613 版本说明书.....8

8 V612 版本说明书.....9

9 V597 版本说明书.....10

10 V596 版本说明书.....11

11 V593 版本说明书.....13

12 V587 版本说明书.....14

13 V586 版本说明书.....16

14 漏洞修补列表.....17

1 V631 版本说明书

发布版本日期

2021-09-04

发布许可版本

V631

上次更新版本

V626

特性描述

- 新增支持 3516 Raid 卡。
- 新增支持 03029TSF 硬盘背板。
- 新增支持 H3200 NVMe 硬盘。
- 新增支持 H3100 NVMe 硬盘。
- 新增支持 D526 1.6T NVMe 硬盘。
- 新增支持 D926 3.2T NVMe 硬盘。
- 新增支持 PM9A3 NVMe 硬盘。
- 新增支持 LPe32000-AP 网卡。
- 新增支持内存故障预测自愈功能。

注意事项

若需使用内存故障预测自愈功能，请配套 BIOS V180 及以上版本。

防病毒扫描说明

见病毒扫描报告。

2 V626 版本说明书

发布版本日期

2021-08-10

发布许可版本

V626

上次更新版本

V625

特性描述

- 增强用户信息可靠性。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

3 V625 版本说明书

发布版本日期

2021-07-27

发布许可版本

V625

上次更新版本

V622

特性描述

- 优化 license 文件导入机制。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

4 V622 版本说明书

发布版本日期

2021-06-08

发布许可版本

V622

上次更新版本

V620

特性描述

- 新增支持 MCX512A-ACUT 网卡。
- 新增支持 MCX515A-CCUT 网卡。
- 新增支持 QLE2692-HUA-SP 网卡。
- 新增支持 QLE2690 网卡。
- 新增支持 QLE2772 网卡。
- 新增支持 QLE2770 网卡。
- 新增支持 RTX 6000 GPU 卡。
- 新增支持 ES3600P V6 6.4T NVMe 硬盘。
- 新增支持 ES3600P V6 1.6T/3.2T NVMe 硬盘。
- 新增支持 ES3500P V6 1.92T/7.68T NVMe 硬盘。
- 新增支持 Seagate Cimarron-BP SATA 硬盘。
- 新增支持 Seagate X18 Evans BP SATA 硬盘。
- 新增支持 ES3500S V6 960GB/1.92TB/3.84TB/7.68TB SAS 硬盘。
- 新增支持 ES3600S V6 3.2TB SAS 硬盘。
- 新增支持 SMI 480GB M.2 转接卡。
- 新增支持可配置防止 DNS 重绑定功能。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

5 V620 版本说明书

发布版本日期

2021-05-08

发布许可版本

V620

上次更新版本

V616

特性描述

- 新增支持 SAS 3152 Raid 卡。
- 新增支持 9440-8i Raid 卡。
- 优化 Redfish 接口响应机制。
- 优化硬盘告警机制。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

6 V616 版本说明书

发布版本日期

2021-03-30

发布许可版本

V616

上次更新版本

V613

特性描述

- 新增支持 Samsung PM1733 EVT2 Nvme 硬盘。
- 优化 IPMI 命令处理机制。
- 升级 OpenLDAP 开源软件补丁，解决（CVE-2020-25692、CVE-2020-36221、CVE-2020-36222、CVE-2020-36223、CVE-2020-36224、CVE-2020-36225、CVE-2020-36226、CVE-2020-36227、CVE-2020-36228、CVE-2020-36229、CVE-2020-36230、CVE-2021-27212）业界已知漏洞。
- 升级 OpenSSH 开源软件补丁，解决（CVE-2020-14145、CVE-2021-28041）业界已知漏洞。
- 优化内存 UCE 告警上报机制。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

7 V613 版本说明书

发布版本日期

2021-02-28

发布许可版本

V613

上次更新版本

V612

特性描述

- 新增支持 T8810 V1 NVMe 硬盘。
- 新增支持 T8830 V1 NVMe 硬盘。
- 新增支持 ES3521 V6 SATA 硬盘。
- 优化 Web 接口一键收集日志文件名（机型名_服务器序列号_年月日-时分）。
- 支持 LADP 服务器 O 标签。
- 优化 CPU 最大支持个数显示机制。
- 升级 Kerberos 补丁，解决（CVE-2020-28196）业界已知漏洞。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

8 V612 版本说明书

发布版本日期

2021-01-21

发布许可版本

V612

上次更新版本

V597

特性描述

- 升级 OpenLdap 补丁，解决（CVE-2020-25692）业界已知漏洞。
- 升级 curl 版本至 7.71.1，解决（CVE-2020-8284、CVE-2020-8285、CVE-2020-8286）业界已知漏洞。
- 升级 SNMP 补丁，解决（CVE-2019-20892）业界已知漏洞。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

9 V597 版本说明书

发布版本日期

2020-12-17

发布许可版本

V597

上次更新版本

V596

特性描述

优化 SNMP Trap 消息上报顺序。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

10 V596 版本说明书

发布版本日期

2020-12-02

发布许可版本

V596

上次更新版本

V593

特性描述

- 优化 BMC 对 CPLD 防护机制。
- 支持网卡顺序按槽位号先后顺序显示。
- 优化 iBMC 访问 NandFlash 机制。
- 优化 CPLD 升级机制。
- 优化更换主板后导入完成提示信息。
- 新增支持 CPU 和整机功耗信息获取。
- 优化 Redfish 事件订阅机制。
- 优化提升 VMM 传输文件速率。
- 优化智能故障管理数据库查询机制。
- 支持 3508 MR 卡。
- 新增支持 JBOD 模式下管理硬盘资源。
- 支持导入 foreign 盘配置到 Raid 卡。
- 新增专用管理网口配置 VLAN 功能。
- IPMI 查询 SEL 显示的时间戳从 GMT 标准时间调整为当地时间。
- 新增支持通过 Redfish 接口启用和禁用夏令时。
- 新增支持 PM6-R 0.96/1.92/3.84/7.68TB 硬盘。
- 新增支持 PM6-V 0.8/1.6/3.2/6.4TB 硬盘。

- 新增支持 PS4510 480GB 硬盘。
- 新增支持 5300pro 240/480/960/1920/3840GB 硬盘。
- 新增支持 5300MAX 240/480/960/1920/3840GB 硬盘。
- 新增支持 T408 GPU PCIe 卡。
- 升级 PCRE 版本至 8.44，解决 cve-2019-20838 安全漏洞。
- 升级 Apache HTTP Server 版本至 2.4.46，解决（CVE-2020-9490）业界已知漏洞。
- 升级 jquery 版本至 3.5.0，解决（CVE-2020-11023）业界已知漏洞。
- 升级 angularjs 版本到 1.8.0，解决（CVE-2020-11022）业界已知漏洞。
- 升级 libjpeg 版本至 9d，解决（CVE-2018-10126、CVE-2018-11813、CVE-2020-14153、CVE-2020-14152）业界已知漏洞。
- 升级 curl 版本至 7.69.1，解决（CVE-2019-5436）业界已知漏洞。
- 升级 NTP - The Network Time Protocol 4.2.8p13 到 NTP - The Network Time Protocol 4.2.8p14，解决（CVE-2019-11331）业界已知漏洞。
- 升级 OpenLDAP 版本至 2.4.49，解决（CVE-2017-9287、CVE-2005-2069、CVE-2017-14159、CVE-2017-17740、CVE-2019-13565、CVE-2019-13057、CVE-2009-3767、CVE-2020-12243、CVE-2015-3276、CVE-2020-15719）业界已知漏洞。
- 升级 Openssh 版本至 8.2p1，解决（CVE-2019-6109、CVE-2019-6110、CVE-2019-6111、CVE-2020-12062）业界已知漏洞。
- 升级 Sqlite 版本到 3.31.1，解决（CVE-2020-13435、CVE-2020-13434、CVE-2020-11656、CVE-2020-11655、CVE-2020-13632、CVE-2020-13630、CVE-2020-13631）业界已知漏洞。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

11 V593 版本说明书

发布版本日期

2020-11-23

发布许可版本

V593

上次更新版本

V587

特性描述

- 新增支持固件包升级描述文件 version.xml 中Vendor 字段值为空。
- 增强 WEB 安全性。
- 新增支持 SP382 网卡。
- 新增支持 MCX653105A-EFAT 网卡。
- 新增支持 MegaRAID 9560-16i 8G RAID 卡。
- 新增支持 PM1733 EVT1 NVMe 硬盘。
- 新增支持 Asen Plus 1.92T/3.84T 硬盘。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

12 V587 版本说明书

发布版本日期

2020-09-02

发布许可版本

V587

上次更新版本

V586

特性描述

- 增强电源功率信息准确性。
- 新增支持 LPE31000-AP FC 网卡。
- 新增支持 LPE31002-AP FC 网卡。
- 新增支持 MCX516A-CCAT NIC 网卡。
- 新增支持 SP380 NIC 网卡。
- 新增支持 PM1725B 1.6/3.2TB NVMe 硬盘。
- 新增支持 PM983 960/1920/3840GB NVMe 硬盘。
- 新增支持 PM1733 1.92/3.84/7.68TB NVMe 硬盘。
- 新增支持 PM1643A 960/1920/3840/7680GB SAS 硬盘。
- 新增支持 MCX515A-CCUT NIC 网卡。
- 新增支持 MCX4121A-XCHT NIC 网卡。
- 新增支持 MCX4121A-ACUT NIC 网卡。
- 新增支持 Micron 7300 PRO 1.92/3.84/7.68 NVMe 硬盘。
- 新增支持 Micron 7300 MAX 1.6/3.2/6.4TB NVMe 硬盘。
- 新增支持 WDC BCQ 3 DWPD SAS 硬盘。

注意事项

NA

13 V586 版本说明书

发布版本日期

2020-08-30

发布许可版本

V586

上次更新版本

NA

特性描述

首次发布

注意事项

NA

14

漏洞修补列表

软件名称	软件版本	CVE 编号	实际 CVSS 得分	漏洞描述	解决版本
curl	7.71.1	CVE-2021-22922	6.5	When curl is instructed to download content using the metalink feature, the contents is verified against a hash provided in the metalink XML file. The metalink XML file points out to the client how to get the same content from a set of different URLs, potentially hosted by different servers and the client can then download the file from one or several of them. In a serial or parallel manner. If one of the servers hosting the contents has been breached and the contents of the specific file on that serv	V631
curl	7.71.1	CVE-2021-22923	5.3	When curl is instructed to get content using the metalink feature, and a user name and password are used to download the metalink XML file, those same credentials are then subsequently passed on to each of the servers from which curl will download or try to download the contents from. Often contrary to the user's expectations and intentions and without telling the user it happened.	V631
curl	7.71.1	CVE-2021-22924	7.4	libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse, if one of them matches the setup. Due to errors in the logic, the config matching function did not take	V631

				'issuercert' into account and it compared the involved paths *case insensitively*, which could lead to libcurl reusing wrong connections. File paths are, or can be, case sensitive on many systems but not all, and can even vary depending on used file systems. The comparison also didn't include the 'issu	
curl	7.71.1	CVE-2021-22925	5.3	curl supports the <code>-t</code> command line option, known as <code>CURLOPT_TELNETOPTIONS</code> in libcurl. This rarely used option is used to send variable=content pairs to TELNET servers. Due to a flaw in the option parser for sending <code>NEW_ENV</code> variables, libcurl could be made to pass on uninitialized data from a stack based buffer to the server. Therefore potentially revealing sensitive internal information to the server using a clear-text network protocol. This could happen because curl did not call and use <code>sscanf()</code>	V631
curl	7.71.1	CVE-2021-22926	7.5	libcurl-using applications can ask for a specific client certificate to be used in a transfer. This is done with the <code>CURLOPT_SSLCERT</code> option (<code>--cert</code> with the command line tool). When libcurl is built to use the macOS native TLS library Secure Transport, an application can ask for the client certificate by name or with a file name - using the same option. If the name exists as a file, it will be used instead of by name. If the application runs with a current working directory that is writable by	V631
Openldap	2.4.58	CVE-2020-25709	7.5	A flaw was found in OpenLDAP. This flaw allows an attacker who can send a malicious packet to be processed by OpenLDAP's slapd server, to trigger an assertion failure. The highest threat from this vulnerability is to system availability.	V631
Openldap	2.4.58	CVE-	7.5	A flaw was found in OpenLDAP in	V631

		2020-25710		versions before 2.4.56. This flaw allows an attacker who sends a malicious packet processed by OpenLDAP to force a failed assertion in csNormalize23(). The highest threat from this vulnerability is to system availability.	
Kernel	4.4	CVE-2020-24587	2.6	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that all fragments of a frame are encrypted under the same key. An adversary can abuse this to decrypt selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP encryption key is periodically renewed.	V631
Kernel	4.4	CVE-2020-24588	3.5	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that the A-MSDU flag in the plaintext QoS header field is authenticated. Against devices that support receiving non-SSP A-MSDU frames (which is mandatory as part of 802.11n), an adversary can abuse this to inject arbitrary network packets.	V631
Kernel	4.4	CVE-2020-26139	5.3	An issue was discovered in the kernel in NetBSD 7.1. An Access Point (AP) forwards EAPOL frames to other clients even though the sender has not yet successfully authenticated to the AP. This might be abused in projected Wi-Fi networks to launch denial-of-service attacks against connected clients and makes it easier to exploit other vulnerabilities in connected clients.	V631
Kernel	4.4	CVE-2020-26140	6.5	An issue was discovered in the ALFA Windows 10 driver 6.1316.1209 for AWUS036H. The WEP, WPA, WPA2, and WPA3 implementations accept plaintext	V631

				frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.	
Kernel	4.4	CVE-2020-26143	6.5	An issue was discovered in the ALFA Windows 10 driver 1030.36.604 for AWUS036ACH. The WEP, WPA, WPA2, and WPA3 implementations accept fragmented plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.	V631
Kernel	4.4	CVE-2020-26141	6.5	An issue was discovered in the ALFA Windows 10 driver 6.1316.1209 for AWUS036H. The Wi-Fi implementation does not verify the Message Integrity Check (authenticity) of fragmented TKIP frames. An adversary can abuse this to inject and possibly decrypt packets in WPA or WPA2 networks that support the TKIP data-confidentiality protocol.	V631
Kernel	4.4	CVE-2020-26146	5.3	An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WPA, WPA2, and WPA3 implementations reassemble fragments with non-consecutive packet numbers. An adversary can abuse this to exfiltrate selected fragments. This vulnerability is exploitable when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used. Note that WEP is vulnerable to this attack by design.	V631
Kernel	4.4	CVE-2020-26145	6.5	An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WEP, WPA, WPA2, and WPA3 implementations accept second (or subsequent) broadcast fragments even when sent in plaintext and process them as full unfragmented frames. An adversary can abuse this to inject arbitrary network packets independent of the network	V631

				configuration.	
Kernel	4.4	CVE-2020-26147	5.4	An issue was discovered in the Linux kernel 5.8.9. The WEP, WPA, WPA2, and WPA3 implementations reassemble fragments even though some of them were sent in plaintext. This vulnerability can be abused to inject packets and/or exfiltrate selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used.	V631
Kernel	4.4	CVE-2020-26144	6.5	An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WEP, WPA, WPA2, and WPA3 implementations accept plaintext A-MSDU frames as long as the first 8 bytes correspond to a valid RFC1042 (i.e., LLC/SNAP) header for EAPOL. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.	V631
Kernel	4.4	CVE-2021-33909	7.8	fs/seq_file.c in the Linux kernel 3.16 through 5.13.x before 5.13.4 does not properly restrict seq buffer allocations, leading to an integer overflow, an Out-of-bounds Write, and escalation to root by an unprivileged user, aka CID-8cae8cd89f05.	V631
Kernel	4.4	CVE-2021-21781	3.3	An information disclosure vulnerability exists in the ARM SIGPAGE functionality of Linux Kernel v5.4.66 and v5.4.54. The latest version (5.11-rc4) seems to still be vulnerable. A userland application can read the contents of the sigpage, which can leak kernel memory contents. An attacker can read a process' s memory at a specific offset to trigger this vulnerability. This was fixed in kernel releases: 4.14.222 4.19.177 5.4.99 5.10.17 5.11	V631
Kernel	4.4	CVE-2021-26930	7.8	An issue was discovered in the Linux kernel 3.11 through 5.10.16, as used by Xen. To service requests to the PV backend, the	V631

				driver maps grant references provided by the frontend. In this process, errors may be encountered. In one case, an error encountered earlier might be discarded by later processing, resulting in the caller assuming successful mapping, and hence subsequent operations trying to access space that wasn't mapped. In another case, internal state would be insufficiently updated,	
Kernel	4.4	CVE-2021-26931	5.5	An issue was discovered in the Linux kernel 2.6.39 through 5.10.16, as used in Xen. Block, net, and SCSI backends consider certain errors a plain bug, deliberately causing a kernel crash. For errors potentially being at least under the influence of guests (such as out of memory conditions), it isn't correct to assume a plain bug. Memory allocations potentially causing such crashes occur only when Linux is running in PV mode, though. This affects drivers/block/xen-blkback/blkback.c and drivers/x	V631
Kernel	4.4	CVE-2021-26932	5.5	An issue was discovered in the Linux kernel 3.2 through 5.10.16, as used by Xen. Grant mapping operations often occur in batch hypercalls, where a number of operations are done in a single hypercall, the success or failure of each one is reported to the backend driver, and the backend driver then loops over the results, performing follow-up actions based on the success or failure of each operation. Unfortunately, when running in PV mode, the Linux backend drivers mishandle this: Some errors are	V631
Kernel	4.4	CVE-2021-27363	4.4	An issue was discovered in the Linux kernel through 5.11.3. A kernel pointer leak can be used to determine the address of the iscsi_transport structure. When an iSCSI transport is registered with the iSCSI subsystem, the transport's handle is available to unprivileged users via the sysfs file system, at /sys/class/iscsi_transport/\$TRANSP	V631

				ORT_NAME/handle. When read, the show_transport_handle function (in drivers/scsi/scsi_transport_iscsi.c) is called, which leaks the handle. This handle is actual	
Kernel	4.4	CVE-2021-27364	7.1	An issue was discovered in the Linux kernel through 5.11.3. drivers/scsi/scsi_transport_iscsi.c is adversely affected by the ability of an unprivileged user to craft Netlink messages.	V631
Kernel	4.4	CVE-2021-28038	6.5	An issue was discovered in the Linux kernel through 5.11.3, as used with Xen PV. A certain part of the netback driver lacks necessary treatment of errors such as failed memory allocations (as a result of changes to the handling of grant mapping errors). A host OS denial of service may occur during misbehavior of a networking frontend driver. NOTE: this issue exists because of an incomplete fix for CVE-2021-26931.	V631
Kernel	4.4	CVE-2021-27365	7.8	An issue was discovered in the Linux kernel through 5.11.3. Certain iSCSI data structures do not have appropriate length constraints or checks, and can exceed the PAGE_SIZE value. An unprivileged user can send a Netlink message that is associated with iSCSI, and has a length up to the maximum length of a Netlink message.	V631
Kernel	4.4	CVE-2021-20261	6.4	A race condition was found in the Linux kernels implementation of the floppy disk drive controller driver software. The impact of this issue is lessened by the fact that the default permissions on the floppy device (/dev/fd0) are restricted to root. If the permissions on the device have changed the impact changes greatly. In the default configuration root (or equivalent) permissions are required to attack this flaw.	V631
Kernel	4.4	CVE-	7.8	rtw_wx_set_scan in drivers/staging	V631

		2021-28660		/rtl8188eu/os_dep/ioctl_linux.c in the Linux kernel through 5.11.6 allows writing beyond the end of the ->ssid[] array. NOTE: from the perspective of kernel.org releases, CVE IDs are not normally used for drivers/staging/* (unfinished work); however, system integrators may have situations in which a drivers/staging issue is relevant to their own customer base.	
Kernel	4.4	CVE-2021-28972	6.7	In drivers/pci/hotplug/rpadlpar_sysfs.c in the Linux kernel through 5.11.8, the RPA PCI Hotplug driver has a user-tolerable buffer overflow when writing a new device name to the driver from userspace, allowing userspace to write data to the kernel stack frame directly. This occurs because add_slot_store and remove_slot_store mishandle drc_name '\0' termination, aka CID-cc7a0bb058b8.	V631
Kernel	4.4	CVE-2020-35519	7.8	An out-of-bounds (OOB) memory access flaw was found in x25_bind in net/x25/af_x25.c in the Linux kernel version v5.12-rc5. A bounds check failure allows a local attacker with a user account on the system to gain access to out-of-bounds memory, leading to a system crash or a leak of internal kernel information. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	V631
Kernel	4.4	CVE-2021-29265	4.7	An issue was discovered in the Linux kernel before 5.11.7. usbip_sockfd_store in drivers/usb/usbip/stub_dev.c allows attackers to cause a denial of service (GPF) because the stub-up sequence has race conditions during an update of the local and shared status, aka CID-9380afd6df70.	V631
Kernel	4.4	CVE-	4.4	Vulnerability Summary for CVE-	V631

		2021-3428		2021-3428	
Kernel	4.4	CVE-2021-28688	6.5	The fix for XSA-365 includes initialization of pointers such that subsequent cleanup code wouldn't use uninitialized or stale values. This initialization went too far and may under certain conditions also overwrite pointers which are in need of cleaning up. The lack of cleanup would result in leaking persistent grants. The leak in turn would prevent fully cleaning up after a respective guest has died, leaving around zombie domains. All Linux versions having the fix for XSA-365 applied are vulne	V631
Kernel	4.4	CVE-2021-30002	6.2	An issue was discovered in the Linux kernel before 5.11.3 when a webcam device exists. video_usercopy in drivers/media/v4l2-core/v4l2-ioc.c has a memory leak for large arguments, aka CID-fb18802a338b.	V631
Kernel	4.4	CVE-2021-29154	7.8	BPF JIT compilers in the Linux kernel through 5.11.12 have incorrect computation of branch displacements, allowing them to execute arbitrary code within the kernel context. This affects arch/x86/net/bpf_jit_comp.c and arch/x86/net/bpf_jit_comp32.c.	V631
Kernel	4.4	CVE-2021-3483	7.8	A flaw was found in the Nosy driver in the Linux kernel. This issue allows a device to be inserted twice into a doubly-linked list, leading to a use-after-free when one of these devices is removed. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. Versions before kernel 5.12-rc6 are affected	V631
Kernel	4.4	CVE-2020-36312	5.5	An issue was discovered in the Linux kernel before 5.8.10. virt/kvm/kvm_main.c has a kvm_io_bus_unregister_dev memory leak upon a kcalloc failure, aka CID-f65886606c2d.	V631

Kernel	4.4	CVE-2021-20292	6.7	There is a flaw reported in the Linux kernel in versions before 5.9 in drivers/gpu/drm/nouveau/nouveau_sgdma.c in nouveau_sgdma_create_ttm in Nouveau DRM subsystem. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker with a local account with a root privilege, can leverage this vulnerability to escalate privileges and execute code in the context of the kernel.	V631
Kernel	4.4	CVE-2020-36322	5.5	An issue was discovered in the FUSE filesystem implementation in the Linux kernel before 5.10.6, aka CID-5d069dbe8aaf. fuse_do_getattr() calls make_bad_inode() in inappropriate situations, causing a system crash. NOTE: the original fix for this vulnerability was incomplete, and its incompleteness is tracked as CVE-2021-28950.	V631
Kernel	4.4	CVE-2020-25670	7.8	A vulnerability was found in Linux Kernel where refcount leak in llcp_sock_bind() causing use-after-free which might lead to privilege escalations.	V631
Kernel	4.4	CVE-2020-25671	7.8	A vulnerability was found in Linux Kernel, where a refcount leak in llcp_sock_connect() causing use-after-free which might lead to privilege escalations.	V631
Kernel	4.4	CVE-2020-25672	7.5	A memory leak vulnerability was found in Linux kernel in llcp_sock_connect	V631
Kernel	4.4	CVE-2020-25673	5.5	A vulnerability was found in Linux kernel where non-blocking socket in llcp_sock_connect() leads to leak and eventually hanging-up the system.	V631
Kernel	4.4	CVE-2021-31916	6.7	An out-of-bounds (OOB) memory write flaw was found in list_devices in drivers/md/dm-ioctl.c in the Multi-device driver module in the Linux kernel before 5.12. A bound check failure allows an attacker	V631

				cker with special user (CAP_SYS_ADMIN) privilege to gain access to out-of-bounds memory leading to a system crash or a leak of internal kernel information. The highest threat from this vulnerability is to system availability.	
Kernel	4.4	CVE-2021-32399	7.0	net/bluetooth/hci_request.c in the Linux kernel through 5.12.2 has a race condition for removal of the HCI controller.	V631
Kernel	4.4	CVE-2021-23134	7.8	Use After Free vulnerability in nfc sockets in the Linux Kernel before 5.12.4 allows local attackers to elevate their privileges. In typical configurations, the issue can only be triggered by a privileged local user with the CAP_NET_RAW capability.	V631
Kernel	4.4	CVE-2021-33034	7.8	In the Linux kernel before 5.12.4, net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan, aka CID-5c4c8c954409. This leads to writing an arbitrary value.	V631
Kernel	4.4	CVE-2021-33033	7.8	The Linux kernel before 5.11.14 has a use-after-free in cipso_v4_genopt in net/ipv4/cipso_ipv4.c because the CIPSO and CALIPSO refcounting for the DOI definitions is mishandled, aka CID-ad5d07f4a9cd. This leads to writing an arbitrary value.	V631
syslog	3.29.1	CVE-2020-8019	7.8	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of syslog-ng of SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Module for Legacy Software 12, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server for SAP 12-SP1; openSUSE Backports SLE-15-SP1, openSUSE Leap 15.1 allowed local attackers controlling	V631

				the user news to escalate their privileges to root. This issue	
Kernel	4.4	CVE-2020-25645	7.8	A flaw was found in the Linux kernel in versions before 5.9-rc7. Traffic between two Geneve endpoints may be unencrypted when IPsec is configured to encrypt traffic for the specific UDP port used by the GENEVE tunnel allowing anyone between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.	V626
Kernel	4.4	CVE-2020-25656	4.1	A flaw was found in the Linux kernel. A use-after-free was found in the way the console subsystem was using ioctl KDGKBSSENT and KDSKBSSENT. 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.	V626
Kernel	4.4	CVE-2020-25705	7.4	A flaw in ICMP packets in the Linux kernel may allow an attacker to quickly scan open UDP ports. This flaw allows an off-path remote attacker to effectively bypass source port UDP randomization. Software that relies on UDP source port randomization are indirectly affected as well on the Linux Based Products (RUGGEDCOM RM1224: All versions between v5.0 and v6.4, SCALANCE M-800: All versions between v5.0 and v6.4, SCALANCE S615: All versions between v5.0 and v6.4, SCALANCE SC-600: All versions pr	V626
Kernel	4.4	CVE-2020-25668	7.0	A flaw was found in Linux Kernel because access to the global variable fg_console is not properly synchronized leading to a use after free in con_font_op.	V626
Kernel	4.4	CVE-2020-8694	5.5	Insufficient access control in the Linux kernel driver for some Intel(R) Processors may allow an authenticated user to potentially	V626

				enable information disclosure via local access.	
Kernel	4.4	CVE-2020-27673	5.5	An issue was discovered in the Linux kernel through 5.9.1, as used with Xen through 4.14.x. Guest OS users can cause a denial of service (host OS hang) via a high rate of events to dom0, aka CID-e99502f76271.	V626
Kernel	4.4	CVE-2020-27675	4.7	An issue was discovered in the Linux kernel through 5.9.1, as used with Xen through 4.14.x. drivers/xen/events/events_base.c allows event-channel removal during the event-handling loop (a race condition). This can cause a use-after-free or NULL pointer dereference, as demonstrated by a dom0 crash via events for an in-reconfiguration paravirtualized device, aka CID-073d0552ead5.	V626
Kernel	4.4	CVE-2020-28915	5.8	A buffer over-read (at the framebuffer layer) in the fbcon code in the Linux kernel before 5.8.15 could be used by local attackers to read kernel memory, aka CID-6735b4632def.	V626
Kernel	4.4	CVE-2020-28974	5.0	A slab-out-of-bounds read in fbcon in the Linux kernel before 5.9.7 could be used by local attackers to read privileged information or potentially crash the kernel, aka CID-3c4e0dff2095. This occurs because KD_FONT_OP_COPY in drivers/tty/vt/vt.c can be used for manipulations such as font height.	V626
Kernel	4.4	CVE-2019-20934	5.3	An issue was discovered in the Linux kernel before 5.2.6. On NUMA systems, the Linux fair scheduler has a use-after-free in show_numa_stats() because NUMA fault statistics are inappropriately freed, aka CID-16d51a590a8c.	V626
Kernel	4.4	CVE-2020-29370	7.0	An issue was discovered in kmem_cache_alloc_bulk in mm/slub.c in the Linux kernel before 5.5.11. The slowpath lacks the required TID increment, aka CID-fd4d9c7d0c71.	V626

Kernel	4.4	CVE-2020-29371	3.3	An issue was discovered in romfs_dev_read in fs/romfs/storage.c in the Linux kernel before 5.8.4. Uninitialized memory leaks to userspace, aka CID-bcf85fcedfdd.	V626
Kernel	4.4	CVE-2020-27786	7.8	A flaw was found in the Linux kernel's implementation of MIDI, where an attacker with a local account and the permissions to issue ioctl commands to midi devices could trigger a use-after-free issue. A write to this specific memory while freed and before use causes the flow of execution to change and possibly allow for memory corruption or privilege escalation. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	V626
Kernel	4.4	CVE-2020-4788	4.7	IBM Power9 (AIX 7.1, 7.2, and VIOS 3.1) processors could allow a local user to obtain sensitive information from the data in the L1 cache under extenuating circumstances. IBM X-Force ID: 189296.	V626
Kernel	4.4	CVE-2020-25669	7.8	A vulnerability was found in the Linux Kernel where the function sunkbd_reinit having been scheduled by sunkbd_interrupt before sunkbd being freed. Though the dangling pointer is set to NULL in sunkbd_disconnect, there is still an alias in sunkbd_reinit causing Use After Free.	V626
Kernel	4.4	CVE-2020-27777	6.7	A flaw was found in the way RTAS handled memory accesses in userspace to kernel communication. On a locked down (usually due to Secure Boot) guest system running on top of PowerVM or KVM hypervisors (pseries platform) a root like local user could use this flaw to further increase their privileges to that of a running kernel.	V626
Kernel	4.4	CVE-2020-29660	4.4	A locking inconsistency issue was discovered in the tty subsystem of the Linux kernel through 5.9.13.	V626

				drivers/tty/tty_io.c and drivers/tty/tty_jobctrl.c may allow a read-after-free attack against TIOCGSID, aka CID-c8bcd9c5be24.	
Kernel	4.4	CVE-2020-29661	7.8	A locking issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP, aka CID-54ffccbf053b.	V626
Kernel	4.4	CVE-2020-0465	6.8	In various methods of hid-multitouch.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-162844689References: Upstream kernel	V626
Kernel	4.4	CVE-2020-29568	6.5	An issue was discovered in Xen through 4.14.x. Some OSes (such as Linux, FreeBSD, and NetBSD) are processing watch events using a single thread. If the events are received faster than the thread is able to handle, they will get queued. As the queue is unbounded, a guest may be able to trigger an OOM in the backend. All systems with a FreeBSD, Linux, or NetBSD (any version) dom0 are vulnerable.	V626
Kernel	4.4	CVE-2020-29569	8.8	An issue was discovered in the Linux kernel through 5.10.1, as used with Xen through 4.14.x. The Linux kernel PV block backend expects the kernel thread handler to reset ring->xenblkd to NULL when stopped. However, the handler may not have time to run if the frontend quickly toggles between the states connect and disconnect. As a consequence, the block backend may re-use a pointer after it was freed. A misbehaving guest can trigger a	V626

				dom0 crash by continuously connecting / disconnecting a block	
Kernel	4.4	CVE-2020-27068	4.4	In the nl80211_policy policy of nl80211.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not required for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-119770583	V626
Kernel	4.4	CVE-2020-0466	7.8	In do_epoll_ctl and ep_loop_check_proc of eventpoll.c, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-147802478References: Upstream kernel	V626
Kernel	4.4	CVE-2020-0444	7.8	In audit_free_lsm_field of auditfilter.c, there is a possible bad kfree due to a logic error in audit_data_to_entry. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-150693166References: Upstream kernel	V626
Kernel	4.4	CVE-2020-27067	6.4	In the l2tp subsystem, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-152409173	V626
Kernel	4.4	CVE-2020-36158	6.7	mwifiex_cmd_802_11_ad_hoc_start in drivers/net/wireless/marvell/mwifiex/join.c in the Linux kernel	V626

				through 5.10.4 might allow remote attackers to execute arbitrary code via a long SSID value, aka CID-5c455c5ab332.	
Kernel	4.4	CVE-2020-27815	7.8	A flaw was found in the JFS filesystem code in the Linux Kernel which allows a local attacker with the ability to set extended attributes to panic the system, causing memory corruption or escalating privileges. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	V626
Kernel	4.4	CVE-2021-3178	6.5	** DISPUTED ** fs/nfsd/nfs3xdr.c in the Linux kernel through 5.10.8, when there is an NFS export of a subdirectory of a filesystem, allows remote attackers to traverse to other parts of the filesystem via READDIRPLUS. NOTE: some parties argue that such a subdirectory export is not intended to prevent this attack; see also the exports(5) no_subtree_check default behavior.	V626
Kernel	4.4	CVE-2020-28374	8.1	In drivers/target/target_core_xcopy.c in the Linux kernel before 5.10.7, insufficient identifier checking in the LIO SCSI target code can be used by remote attackers to read or write files via directory traversal in an XCOPY request, aka CID-2896c93811e3. For example, an attack can occur over a network if the attacker has access to one iSCSI LUN. The attacker gains control over file access because I/O operations are proxied via an attacker-selected backstore.	V626
Kernel	4.4	CVE-2021-3347	7.8	An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.	V626
curl	7.71.1	CVE-	3.7	This candidate has been reserved	V622

		2021-22898		by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.	
curl	7.71.1	CVE-2021-22897	3.7	This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.	V622
underscore	1.9.2	CVE-2021-23358	7.2	The package underscore from 1.13.0-0 and before 1.13.0-2, from 1.3.2 and before 1.12.1 are vulnerable to Arbitrary Code Injection via the template function, particularly when a variable property is passed as an argument as it is not sanitized.	V622
SQLite	3.32.1	CVE-2021-20227	5.5	A flaw was found in SQLite's SELECT query functionality (src/select.c). This flaw allows an attacker who is capable of running SQL queries locally on the SQLite database to cause a denial of service or possible code execution by triggering a use-after-free. The highest threat from this vulnerability is to system availability.	V616
lldpd	1.0.4	CVE-2020-27827	7.5	A flaw was found in multiple versions of OpenvSwitch. Specially crafted LLDP packets can cause memory to be lost when allocating data to handle specific optional TLVs, potentially causing a denial of service. The highest threat from this vulnerability is to system availability.	V616
OpenLDAP	2.4.50	CVE-2020-25692	7.5	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.	V616

OpenLDAP	2.4.50	CVE-2020-36221	7.5	An integer underflow was discovered in OpenLDAP before 2.4.57 leading to slapd crashes in the Certificate Exact Assertion processing, resulting in denial of service (schema_init.c serialNumberAndIssuerCheck).	V616
OpenLDAP	2.4.50	CVE-2020-36222	7.5	A flaw was discovered in OpenLDAP before 2.4.57 leading to an assertion failure in slapd in the saslAuthzTo validation, resulting in denial of service.	V616
OpenLDAP	2.4.50	CVE-2020-36223	7.5	A flaw was discovered in OpenLDAP before 2.4.57 leading to a slapd crash in the Values Return Filter control handling, resulting in denial of service (double free and out-of-bounds read).	V616
OpenLDAP	2.4.50	CVE-2020-36224	7.5	A flaw was discovered in OpenLDAP before 2.4.57 leading to an invalid pointer free and slapd crash in the saslAuthzTo processing, resulting in denial of service.	V616
OpenLDAP	2.4.50	CVE-2020-36225	7.5	A flaw was discovered in OpenLDAP before 2.4.57 leading to a double free and slapd crash in the saslAuthzTo processing, resulting in denial of service.	V616
OpenLDAP	2.4.50	CVE-2020-36226	7.5	A flaw was discovered in OpenLDAP before 2.4.57 leading to a memch->bv_len miscalculation and slapd crash in the saslAuthzTo processing, resulting in denial of service	V616
OpenLDAP	2.4.50	CVE-2020-36227	7.5	A flaw was discovered in OpenLDAP before 2.4.57 leading to an infinite loop in slapd with the cancel_extop Cancel operation, resulting in denial of service.	V616
OpenLDAP	2.4.50	CVE-2020-36228	7.5	An integer underflow was discovered in OpenLDAP before 2.4.57 leading to a slapd crash in the Certificate List Exact Assertion processing, resulting in denial of service.	V616
OpenLDAP	2.4.50	CVE-2020-	7.5	A flaw was discovered in ldap_X509dn2bv in OpenLDAP	V616

		36229		before 2.4.57 leading to a slapd crash in the X.509 DN parsing in ad_keystring, resulting in denial of service.	
OpenLDAP	2.4.50	CVE-2020-36230	7.5	A flaw was discovered in OpenLDAP before 2.4.57 leading in an assertion failure in slapd in the X.509 DN parsing in decode.c ber_next_element, resulting in denial of service.	V616
OpenLDAP	2.4.50	CVE-2021-27212	7.5	In OpenLDAP through 2.4.57 and 2.5.x through 2.5.1alpha, an assertion failure in slapd can occur in the issuerAndThisUpdateCheck function via a crafted packet, resulting in a denial of service (daemon exit) via a short timestamp. This is related to schema_init.c and checkTime.	V616
OpenSSH	8.2p1	CVE-2020-14145	5.9	The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client).	V616
OpenSSH	8.2p1	CVE-2021-28041	7.1	ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.	V616
Kerberos 5	1.18.2	CVE-2020-28196	7.5	MIT Kerberos 5 (aka krb5) before 1.17.2 and 1.18.x before 1.18.3 allows unbounded recursion via an ASN.1-encoded Kerberos message because the lib/krb5/asn.1/asn1_encode.c support for BER indefinite lengths lacks a recursion limit.	V613
OpenLDAP	2.4.50	CVE-2020-25692	7.5	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	V612

				pecially crafted request, causing a Denial of Service.	
curl	7.69.1	CVE-2020-8284	3.7	A malicious server can use the FTP PASV response to trick curl 7.73.0 and earlier into connecting back to a given IP address and port, and this way potentially make curl extract information about services that are otherwise private and not disclosed, for example doing port scanning and service banner extractions.	V612
curl	7.69.1	CVE-2020-8285	7.5	curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wildcard match parsing.	V612
curl	7.69.1	CVE-2020-8286	7.5	curl 7.41.0 through 7.73.0 is vulnerable to an improper check for certificate revocation due to insufficient verification of the OCSP response.	V612
snmp	5.8	CVE-2019-20892	6.5	net-snmp before 5.8.1.pre1 has a double free in usm_free_usmStateReference in snmplib/snmpusm.c via an SNMPv3 GetBulk request. NOTE: this affects net-snmp packages shipped to end users by multiple Linux distributions, but might not affect an upstream release.	V612
PCRE	8.42	CVE-2019-20838	7.5	libpcre in PCRE before 8.43 allows a subject buffer over-read in JIT when UTF is disabled, and \X or \R has more than one fixed quantifier, a related issue to CVE-2019-20454.	V596
Apache HTTP Server	2.4.39	CVE-2020-9490	7.5	Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.	V596
jQuery	3.3.1	CVE-2020-11023	6.1	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing	V596

				<option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0	
jQuery	3.3.1	CVE-2020-11022	6.1	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	V596
libjpeg	9c	CVE-2018-10126	6.5	LibTIFF 4.0.9 has a NULL pointer dereference in the jpeg_fdct_16x16 function in jfdctint.c.	V596
libjpeg	9c	CVE-2018-11813	7.5	libjpeg 9c has a large loop because read_pixel in rdtarga.c mishandles EOF.	V596
libjpeg	9c	CVE-2020-14153	7.1	In IJG JPEG (aka libjpeg) from version 8 through 9c, jdhuft.c has an out-of-bounds array read for certain table pointers.	V596
libjpeg	9c	CVE-2020-14152	7.1	In IJG JPEG (aka libjpeg) before 9d, jpeg_mem_available() in jmemnobs.c in djpeg does not honor the max_memory_to_use setting, possibly causing excessive memory consumption.	V596
curl	7.56.1	CVE-2019-5436	7.8	A heap buffer overflow in the TFTP receiving code allows for DoS or arbitrary code execution in libcurl versions 7.19.4 through 7.64.1.	V596
NTP	4.2.8p13	CVE-2019-11331	8.1	Network Time Protocol (NTP), as specified in RFC 5905, uses port 123 even for modes where a fixed port number is not required, which makes it easier for remote attackers to conduct off-path attacks.	V596
OpenLDAP	2.4.48	CVE-2017-9287	6.5	servers/slapd/back-mdb/search.c in OpenLDAP through 2.4.44 is prone to a double free	V596

				vulnerability. A user with access to search the directory can crash slapd by issuing a search including the Paged Results control with a page size of 0.	
OpenLDAP	2.4.48	CVE-2005-2069	5.0	pam_ldap and nss_ldap, when used with OpenLDAP and connecting to a slave using TLS, does not use TLS for the subsequent connection if the client is referred to a master, which may cause a password to be sent in cleartext and allows remote attackers to sniff the password.	V596
OpenLDAP	2.4.48	CVE-2017-14159	4.7	slapd in OpenLDAP 2.4.45 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill `cat /pathname`" command, as demonstrated by openldap-initscript.	V596
OpenLDAP	2.4.48	CVE-2017-17740	7.5	contrib/slapd-modules/nops/nops.c in OpenLDAP through 2.4.45, when both the nops module and the memberof overlay are enabled, attempts to free a buffer that was allocated on the stack, which allows remote attackers to cause a denial of service (slapd crash) via a member MODDN operation.	V596
OpenLDAP	2.4.48	CVE-2019-13565	7.5	An issue was discovered in OpenLDAP 2.x before 2.4.48. When using SASL authentication and session encryption, and relying on the SASL security layers in slapd access controls, it is possible to obtain access that would otherwise be denied via a simple bind for any identity covered in those ACLs. After the first SASL bind is completed, the sasl_ssf value is retained for all new non-SASL connections. Depending on the ACL configuration, this can affect different types of operations (searches, modi	V596
OpenLDAP	2.4.48	CVE-2019-	4.9	An issue was discovered in the server in OpenLDAP before	V596

		13057		2.4.48. When the server administrator delegates rootDN (database admin) privileges for certain databases but wants to maintain isolation (e.g., for multi-tenant deployments), slapd does not properly stop a rootDN from requesting authorization as an identity from another database during a SASL bind or with a proxyAuthz (RFC 4370) control. (It is not a common configuration to deploy a system where the server administrator and a DB administr	
OpenLDAP	2.4.48	CVE-2009-3767	4.3	libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	V596
OpenLDAP	2.4.48	CVE-2020-12243	7.5	In filter.c in slapd in OpenLDAP before 2.4.50, LDAP search filters with nested boolean expressions can result in denial of service (daemon crash).	V596
OpenLDAP	2.4.48	CVE-2015-3276	5.0	The nss_parse_ciphers function in libraries/libldap/tls_m.c in OpenLDAP does not properly parse OpenSSL-style multi-keyword mode cipher strings, which might cause a weaker than intended cipher to be used and allow remote attackers to have unspecified impact via unknown vectors.	V596
OpenLDAP	2.4.48	CVE-2020-15719	4.2	libldap in certain third-party OpenLDAP packages has a certificate-validation flaw when the third-party package is asserting RFC6125 support. It considers CN even when there is a non-matching subjectAltName (SAN). This is fixed in, for example, openldap-2.4.46-10.el8 in Red Hat	V596

				Enterprise Linux.	
OpenSSH	7.6p1	CVE-2019-6109	6.8	An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.	V596
OpenSSH	7.6p1	CVE-2019-6110	6.8	In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.	V596
OpenSSH	7.6p1	CVE-2019-6111	5.9	An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirect	V596
OpenSSH	7.6p1	CVE-2020-12062	7.5	** DISPUTED ** The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that	V596

SQLite	3.30.1	CVE-2020-13435	5.5	SQLite through 3.32.0 has a segmentation fault in <code>sqlite3ExprCodeTarget</code> in <code>expr.c</code> .	V596
SQLite	3.30.1	CVE-2020-13434	5.5	SQLite through 3.32.0 has an integer overflow in <code>sqlite3_str_vappendf</code> in <code>printf.c</code> .	V596
SQLite	3.30.1	CVE-2020-11656	9.8	In SQLite through 3.31.1, the ALTER TABLE implementation has a use-after-free, as demonstrated by an ORDER BY clause that belongs to a compound SELECT statement.	V596
SQLite	3.30.1	CVE-2020-11655	7.5	SQLite through 3.31.1 allows attackers to cause a denial of service (segmentation fault) via a malformed window-function query because the <code>AggInfo</code> object's initialization is mishandled.	V596
SQLite	3.30.1	CVE-2020-13632	5.5	<code>ext/fts3/fts3_snippet.c</code> in SQLite before 3.32.0 has a NULL pointer dereference via a crafted <code>matchinfo()</code> query.	V596
SQLite	3.30.1	CVE-2020-13630	7.0	<code>ext/fts3/fts3.c</code> in SQLite before 3.32.0 has a use-after-free in <code>fts3EvalNextRow</code> , related to the snippet feature.	V596
SQLite	3.30.1	CVE-2020-13631	5.5	SQLite before 3.32.0 allows a virtual table to be renamed to the name of one of its shadow tables, related to <code>alter.c</code> and <code>build.c</code> .	V596
SQLite	3.30.1	CVE-2020-9327	7.5	In SQLite 3.31.1, <code>isAuxiliaryVtabOperator</code> allows attackers to trigger a NULL pointer dereference and segmentation fault because of generated column optimizations.	V586
SQLite	3.30.1	CVE-2020-11655	7.5	SQLite through 3.31.1 allows attackers to cause a denial of service (segmentation fault) via a malformed window-function query because the <code>AggInfo</code> object's initialization is mishandled.	V586
SQLite	3.30.1	CVE-2020-11656	9.8	In SQLite through 3.31.1, the ALTER TABLE implementation has a use-after-free, as demonstrated by an ORDER BY clause that belongs to a compound SELECT statement.	V586

SQLite	3.30.1	CVE-2020-13435	5.5	SQLite through 3.32.0 has a segmentation fault in sqlite3ExprCodeTarget in expr.c.	V586
SQLite	3.30.1	CVE-2020-13434	5.5	SQLite through 3.32.0 has an integer overflow in sqlite3_str_vappendf in printf.c.	V586
SQLite	3.30.1	CVE-2020-13632	5.5	ext/fts3/fts3_snippet.c in SQLite before 3.32.0 has a NULL pointer dereference via a crafted matchinfo() query	V586
SQLite	3.30.1	CVE-2020-13631	5.5	SQLite before 3.32.0 allows a virtual table to be renamed to the name of one of its shadow tables, related to alter.c and build.c.	V586
SQLite	3.30.1	CVE-2020-13630	7.0	ext/fts3/fts3.c in SQLite before 3.32.0 has a use-after-free in fts3EvalNextRow, related to the snippet feature.	V586
SQLite	3.30.1	CVE-2020-13871	7.5	SQLite 3.32.2 has a use-after-free in resetAccumulator in select.c because the parse tree rewrite for window functions is too late.	V586