Security Advisories 4.5

This page shows the package changes from 4.4 to 4.5 some for security reasons and the CVEs.

Deliverable	Name
netboot	esi-4.5

CVEs and the new package and RPM that resolves each

CVE	New RPM	PKG	DESCRIPTION
CVE-2021-45417	aide-0.15.1-13.el7_9.1.x86_64	aide	AIDE before 0.17.4 allows local users to obtain root privileges via crafted file metadata (such as XFS extended attributes or tmpfs ACLs), because of a heap-based buffer overflow.
CVE-2022-22823	expat-2.1.0-14.el7_9.x86_64	expat	build_model in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-22824	expat-2.1.0-14.el7_9.x86_64	expat	defineAttribute in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-22827	expat-2.1.0-14.el7_9.x86_64	expat	storeAtts in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-25315	expat-2.1.0-14.el7_9.x86_64	expat	In Expat (aka libexpat) before 2.4.5, there is an integer overflow in storeRawNames.
CVE-2022-25235	expat-2.1.0-14.el7_9.x86_64	expat	xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for whether a UTF-8 character is valid in a certain context.
CVE-2022-22825	expat-2.1.0-14.el7_9.x86_64	expat	lookup in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-23852	expat-2.1.0-14.el7_9.x86_64	expat	Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_CONTEXT_BYTES.
CVE-2021-46143	expat-2.1.0-14.el7_9.x86_64	expat	In doProlog in xmlparse.c in Expat (aka libexpat) before 2.4.3, an integer overflow exists for m_groupSize.
CVE-2022-25236	expat-2.1.0-14.el7_9.x86_64	expat	xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert namespace-separator characters into namespace URIs.
CVE-2021-45960	expat-2.1.0-14.el7_9.x86_64	expat	In Expat (aka libexpat) before 2.4.3, a left shift by 29 (or more) places in the storeAtts function in xmlparse.c can lead to realloc misbehavior (e.g., allocating too few bytes, or only freeing memory).

CVE-2022-22822	expat-2.1.0-14.el7_9.x86_64	expat	addBinding in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-22826	expat-2.1.0-14.el7_9.x86_64	expat	nextScaffoldPart in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2021-22555	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through user name space
CVE-2021-22555	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through user name space
CVE-2021-22555	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through user name space
CVE-2021-22555	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through user name space
CVE-2021-22555	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through user name space
CVE-2021-22555	perf-3.10.0-1160.59.1.el7.x86_64	perf	A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through user name space
CVE-2021-0920	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	In unix_scm_to_skb of af_unix.c, there is a possible use after free bug 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-196926917References: Upstream kernel
CVE-2021-0920	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	In unix_scm_to_skb of af_unix.c, there is a possible use after free bug 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-196926917References: Upstream kernel
CVE-2021-0920	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	In unix_scm_to_skb of af_unix.c, there is a possible use after free bug 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-196926917References: Upstream kernel
CVE-2021-0920	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	In unix_scm_to_skb of af_unix.c, there is a possible use after free bug 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-196926917References: Upstream kernel
CVE-2021-0920	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	In unix_scm_to_skb of af_unix.c, there is a possible use after free bug 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-196926917References: Upstream kernel

CVE-2021-0920	perf-3.10.0-1160.59.1.el7.x86_64	perf	In unix_scm_to_skb of af_unix.c, there is a possible use after free bug 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-196926917References: Upstream kernel
CVE-2021-3656	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "virt_ext" field, this issue could allow a malicious L1 to disable both VMLOAD/VMSAVE intercepts and VLS (Virtual VMLOAD/VMSAVE) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape.
CVE-2021-3656	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "virt_ext" field, this issue could allow a malicious L1 to disable both VMLOAD/VMSAVE intercepts and VLS (Virtual VMLOAD/VMSAVE) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape.
CVE-2021-3656	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "virt_ext" field, this issue could allow a malicious L1 to disable both VMLOAD/VMSAVE intercepts and VLS (Virtual VMLOAD/VMSAVE) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape.
CVE-2021-3656	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "virt_ext" field, this issue could allow a malicious L1 to disable both VMLOAD/VMSAVE intercepts and VLS (Virtual VMLOAD/VMSAVE) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape.
CVE-2021-3656	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "virt_ext" field, this issue could allow a malicious L1 to disable both VMLOAD/VMSAVE intercepts and VLS (Virtual VMLOAD/VMSAVE) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape.
CVE-2021-3656	perf-3.10.0-1160.59.1.el7.x86_64	perf	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "virt_ext" field, this issue could allow a malicious L1 to disable both VMLOAD/VMSAVE intercepts and VLS (Virtual VMLOAD/VMSAVE) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape.
CVE-2022-22942	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	• 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.
CVE-2022-22942	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	• 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.
CVE-2022-22942	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	• 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.
CVE-2022-22942	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	• 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.
CVE-2022-22942	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	• 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.
CVE-2022-22942	perf-3.10.0-1160.59.1.el7.x86_64	perf	• 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.

CVE-2021-3573	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	A use-after-free in function hci_sock_bound_ioctl() of the Linux kernel HCI subsystem was found in the way user calls ioct HCIUNBLOCKADDR or other way triggers race condition of the call hci_unregister_dev() together with one of the calls hci_sock_blacklist_add(), hci_sock_blacklist_del(), hci_get_conn_info(), hci_get_auth_info(). A privileged local user could use this flaw to crash the system or escalate their privileges on the system. This flaw affects the Linux kernel versions prior to 5.13-rc5.
CVE-2021-3573	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	A use-after-free in function hci_sock_bound_ioctl() of the Linux kernel HCI subsystem was found in the way user calls ioct HCIUNBLOCKADDR or other way triggers race condition of the call hci_unregister_dev() together with one of the calls hci_sock_blacklist_add(), hci_sock_blacklist_del(), hci_get_conn_info(), hci_get_auth_info(). A privileged local user could use this flaw to crash the system or escalate their privileges on the system. This flaw affects the Linux kernel versions prior to 5.13-rc5.
CVE-2021-3573	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	A use-after-free in function hci_sock_bound_ioctl() of the Linux kernel HCI subsystem was found in the way user calls ioct HCIUNBLOCKADDR or other way triggers race condition of the call hci_unregister_dev() together with one of the calls hci_sock_blacklist_add(), hci_sock_blacklist_del(), hci_get_conn_info(), hci_get_auth_info(). A privileged local user could use this flaw to crash the system or escalate their privileges on the system. This flaw affects the Linux kernel versions prior to 5.13-rc5.
CVE-2021-3573	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	A use-after-free in function hci_sock_bound_ioctl() of the Linux kernel HCI subsystem was found in the way user calls ioct HCIUNBLOCKADDR or other way triggers race condition of the call hci_unregister_dev() together with one of the calls hci_sock_blacklist_add(), hci_sock_blacklist_del(), hci_get_conn_info(), hci_get_auth_info(). A privileged local user could use this flaw to crash the system or escalate their privileges on the system. This flaw affects the Linux kernel versions prior to 5.13-rc5.
CVE-2021-3573	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	A use-after-free in function hci_sock_bound_ioctl() of the Linux kernel HCI subsystem was found in the way user calls ioct HCIUNBLOCKADDR or other way triggers race condition of the call hci_unregister_dev() together with one of the calls hci_sock_blacklist_add(), hci_sock_blacklist_del(), hci_get_conn_info(), hci_get_auth_info(). A privileged local user could use this flaw to crash the system or escalate their privileges on the system. This flaw affects the Linux kernel versions prior to 5.13-rc5.
CVE-2021-3573	perf-3.10.0-1160.59.1.el7.x86_64	perf	A use-after-free in function hci_sock_bound_ioctl() of the Linux kernel HCI subsystem was found in the way user calls ioct HCIUNBLOCKADDR or other way triggers race condition of the call hci_unregister_dev() together with one of the calls hci_sock_blacklist_add(), hci_sock_blacklist_del(), hci_get_conn_info(), hci_get_auth_info(). A privileged local user could use this flaw to crash the system or escalate their privileges on the system. This flaw affects the Linux kernel versions prior to 5.13-rc5.
CVE-2019-20934	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	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.
CVE-2019-20934	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	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.
CVE-2019-20934	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	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.
CVE-2019-20934	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	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.
CVE-2019-20934	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	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.
CVE-2019-20934	perf-3.10.0-1160.59.1.el7.x86_64	perf	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.
CVE-2021-42739	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	A heap-based buffer overflow flaw was found in the Linux kernel FireDTV media card driver, where the user calls the CA_SEND_MSG ioctl. This flaw allows a local user of the host machine to crash the system or escalate privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.

CVE-2021-42739	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	A heap-based buffer overflow flaw was found in the Linux kernel FireDTV media card driver, where the user calls the CA_SEND_MSG ioctl. This flaw allows a local user of the host machine to crash the system or escalate privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2021-42739	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	A heap-based buffer overflow flaw was found in the Linux kernel FireDTV media card driver, where the user calls the CA_SEND_MSG ioctl. This flaw allows a local user of the host machine to crash the system or escalate privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2021-42739	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	A heap-based buffer overflow flaw was found in the Linux kernel FireDTV media card driver, where the user calls the CA_SEND_MSG ioctl. This flaw allows a local user of the host machine to crash the system or escalate privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2021-42739	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	A heap-based buffer overflow flaw was found in the Linux kernel FireDTV media card driver, where the user calls the CA_SEND_MSG ioctl. This flaw allows a local user of the host machine to crash the system or escalate privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2021-42739	perf-3.10.0-1160.59.1.el7.x86_64	perf	A heap-based buffer overflow flaw was found in the Linux kernel FireDTV media card driver, where the user calls the CA_SEND_MSG ioctl. This flaw allows a local user of the host machine to crash the system or escalate privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2021-37576	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	arch/powerpc/kvm/book3s_rtas.c in the Linux kernel through 5.13.5 on the powerpc platform allows KVM guest OS users to cause host OS memory corruption via rtas_args.nargs, aka CID-f62f3c20647e.
CVE-2021-37576	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	arch/powerpc/kvm/book3s_rtas.c in the Linux kernel through 5.13.5 on the powerpc platform allows KVM guest OS users to cause host OS memory corruption via rtas_args.nargs, aka CID-f62f3c20647e.
CVE-2021-37576	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	arch/powerpc/kvm/book3s_rtas.c in the Linux kernel through 5.13.5 on the powerpc platform allows KVM guest OS users to cause host OS memory corruption via rtas_args.nargs, aka CID-f62f3c20647e.
CVE-2021-37576	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	arch/powerpc/kvm/book3s_rtas.c in the Linux kernel through 5.13.5 on the powerpc platform allows KVM guest OS users to cause host OS memory corruption via rtas_args.nargs, aka CID-f62f3c20647e.
CVE-2021-37576	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	arch/powerpc/kvm/book3s_rtas.c in the Linux kernel through 5.13.5 on the powerpc platform allows KVM guest OS users to cause host OS memory corruption via rtas_args.nargs, aka CID-f62f3c20647e.
CVE-2021-37576	perf-3.10.0-1160.59.1.el7.x86_64	perf	arch/powerpc/kvm/book3s_rtas.c in the Linux kernel through 5.13.5 on the powerpc platform allows KVM guest OS users to cause host OS memory corruption via rtas_args.nargs, aka CID-f62f3c20647e.
CVE-2021-33034	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	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.
CVE-2021-33034	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	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.

CVE-2021-33034	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	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.
CVE-2021-33034	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	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.
CVE-2021-33034	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	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.
CVE-2021-33034	perf-3.10.0-1160.59.1.el7.x86_64	perf	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.
CVE-2020-27777	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	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.
CVE-2020-27777	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	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.
CVE-2020-27777	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	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.
CVE-2020-27777	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	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.
CVE-2020-27777	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	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.
CVE-2020-27777	perf-3.10.0-1160.59.1.el7.x86_64	perf	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.
CVE-2020-0465	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	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
CVE-2020-0465	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	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
CVE-2020-0465	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	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

CVE-2020-0465	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	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
CVE-2020-0465	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	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
CVE-2020-0465	perf-3.10.0-1160.59.1.el7.x86_64	perf	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
CVE-2020-0466	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	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
CVE-2020-0466	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	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
CVE-2020-0466	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	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
CVE-2020-0466	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	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
CVE-2020-0466	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	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
CVE-2020-0466	perf-3.10.0-1160.59.1.el7.x86_64	perf	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
CVE-2020-11668	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.
CVE-2020-11668	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.
CVE-2020-11668	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.
CVE-2020-11668	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.

CVE-2020-11668	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.
CVE-2020-11668	perf-3.10.0-1160.59.1.el7.x86_64	perf	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.
CVE-2021-3653	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "int_ctl" field, this issue could allow a malicious L1 to enable AVIC support (Advanced Virtual Interrupt Controller) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape. This flaw affects Linux kernel versions prior to 5.14-rc7.
CVE-2021-3653	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "int_ctl" field, this issue could allow a malicious L1 to enable AVIC support (Advanced Virtual Interrupt Controller) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape. This flaw affects Linux kernel versions prior to 5.14-rc7.
CVE-2021-3653	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "int_ctl" field, this issue could allow a malicious L1 to enable AVIC support (Advanced Virtual Interrupt Controller) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape. This flaw affects Linux kernel versions prior to 5.14-rc7.
CVE-2021-3653	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "int_ctl" field, this issue could allow a malicious L1 to enable AVIC support (Advanced Virtual Interrupt Controller) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape. This flaw affects Linux kernel versions prior to 5.14-rc7.
CVE-2021-3653	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "int_ctl" field, this issue could allow a malicious L1 to enable AVIC support (Advanced Virtual Interrupt Controller) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape. This flaw affects Linux kernel versions prior to 5.14-rc7.
CVE-2021-3653	perf-3.10.0-1160.59.1.el7.x86_64	perf	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "int_ctl" field, this issue could allow a malicious L1 to enable AVIC support (Advanced Virtual Interrupt Controller) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape. This flaw affects Linux kernel versions prior to 5.14-rc7.
CVE-2020-36385	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	An issue was discovered in the Linux kernel before 5.10. drivers/infiniband/core/ucma.c has a use-after-free because the ctx is reached via the ctx_list in some ucma_migrate_id situations where ucma_close is called, aka CID-f5449e74802c.
CVE-2020-36385	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	An issue was discovered in the Linux kernel before 5.10. drivers/infiniband/core/ucma.c has a use-after-free because the ctx is reached via the ctx_list in some ucma_migrate_id situations where ucma_close is called, aka CID-f5449e74802c.
CVE-2020-36385	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	An issue was discovered in the Linux kernel before 5.10. drivers/infiniband/core/ucma.c has a use-after-free because the ctx is reached via the ctx_list in some ucma_migrate_id situations where ucma_close is called, aka CID-f5449e74802c.
CVE-2020-36385	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	An issue was discovered in the Linux kernel before 5.10. drivers/infiniband/core/ucma.c has a use-after-free because the ctx is reached via the ctx_list in some ucma_migrate_id situations where ucma_close is called, aka CID-f5449e74802c.
CVE-2020-36385	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	An issue was discovered in the Linux kernel before 5.10. drivers/infiniband/core/ucma.c has a use-after-free because the ctx is reached via the ctx_list in some ucma_migrate_id situations where ucma_close is called, aka CID-f5449e74802c.

CVE-2020-36385	perf-3.10.0-1160.59.1.el7.x86_64	perf	An issue was discovered in the Linux kernel before 5.10. drivers/infiniband/core/ucma.c has a use-after-free because the ctx is reached via the ctx_list in some ucma_migrate_id situations where ucma_close is called, aka CID-f5449e74802c.
CVE-2021-3564	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	A flaw double-free memory corruption in the Linux kernel HCI device initialization subsystem was found in the way user attach malicious HCI TTY Bluetooth device. A local user could use this flaw to crash the system. This flaw affects all the Linux kernel versions starting from 3.13.
CVE-2021-3564	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	A flaw double-free memory corruption in the Linux kernel HCI device initialization subsystem was found in the way user attach malicious HCI TTY Bluetooth device. A local user could use this flaw to crash the system. This flaw affects all the Linux kernel versions starting from 3.13.
CVE-2021-3564	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	A flaw double-free memory corruption in the Linux kernel HCI device initialization subsystem was found in the way user attach malicious HCI TTY Bluetooth device. A local user could use this flaw to crash the system. This flaw affects all the Linux kernel versions starting from 3.13.
CVE-2021-3564	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	A flaw double-free memory corruption in the Linux kernel HCI device initialization subsystem was found in the way user attach malicious HCI TTY Bluetooth device. A local user could use this flaw to crash the system. This flaw affects all the Linux kernel versions starting from 3.13.
CVE-2021-3564	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	A flaw double-free memory corruption in the Linux kernel HCI device initialization subsystem was found in the way user attach malicious HCI TTY Bluetooth device. A local user could use this flaw to crash the system. This flaw affects all the Linux kernel versions starting from 3.13.
CVE-2021-3564	perf-3.10.0-1160.59.1.el7.x86_64	perf	A flaw double-free memory corruption in the Linux kernel HCI device initialization subsystem was found in the way user attach malicious HCI TTY Bluetooth device. A local user could use this flaw to crash the system. This flaw affects all the Linux kernel versions starting from 3.13.
CVE-2021-29650	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	An issue was discovered in the Linux kernel before 5.11.11. The netfilter subsystem allows attackers to cause a denial of service (panic) because net/netfilter/x_tables.c and include/linux/netfilter/x_tables.h lack a full memory barrier upon the assignment of a new table value, aka CID-175e476b8cdf.
CVE-2021-29650	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	An issue was discovered in the Linux kernel before 5.11.11. The netfilter subsystem allows attackers to cause a denial of service (panic) because net/netfilter/x_tables.c and include/linux/netfilter/x_tables.h lack a full memory barrier upon the assignment of a new table value, aka CID-175e476b8cdf.
CVE-2021-29650	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	An issue was discovered in the Linux kernel before 5.11.11. The netfilter subsystem allows attackers to cause a denial of service (panic) because net/netfilter/x_tables.c and include/linux/netfilter/x_tables.h lack a full memory barrier upon the assignment of a new table value, aka CID-175e476b8cdf.
CVE-2021-29650	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	An issue was discovered in the Linux kernel before 5.11.11. The netfilter subsystem allows attackers to cause a denial of service (panic) because net/netfilter/x_tables.c and include/linux/netfilter/x_tables.h lack a full memory barrier upon the assignment of a new table value, aka CID-175e476b8cdf.
CVE-2021-29650	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	An issue was discovered in the Linux kernel before 5.11.11. The netfilter subsystem allows attackers to cause a denial of service (panic) because net/netfilter/x_tables.c and include/linux/netfilter/x_tables.h lack a full memory barrier upon the assignment of a new table value, aka CID-175e476b8cdf.
CVE-2021-29650	perf-3.10.0-1160.59.1.el7.x86_64	perf	An issue was discovered in the Linux kernel before 5.11.11. The netfilter subsystem allows attackers to cause a denial of service (panic) because net/netfilter/x_tables.c and include/linux/netfilter/x_tables.h lack a full memory barrier upon the assignment of a new table value, aka CID-175e476b8cdf.

CVE-2022-0330	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	A random memory access flaw was found in the Linux kernel's GPU i915 kernel driver functionality in the way a user may run malicious code on the GPU. This flaw allows a local user to crash the system or escalate their privileges on the system.
CVE-2022-0330	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	A random memory access flaw was found in the Linux kernel's GPU i915 kernel driver functionality in the way a user may run malicious code on the GPU. This flaw allows a local user to crash the system or escalate their privileges on the system.
CVE-2022-0330	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	A random memory access flaw was found in the Linux kernel's GPU i915 kernel driver functionality in the way a user may run malicious code on the GPU. This flaw allows a local user to crash the system or escalate their privileges on the system.
CVE-2022-0330	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	A random memory access flaw was found in the Linux kernel's GPU i915 kernel driver functionality in the way a user may run malicious code on the GPU. This flaw allows a local user to crash the system or escalate their privileges on the system.
CVE-2022-0330	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	A random memory access flaw was found in the Linux kernel's GPU i915 kernel driver functionality in the way a user may run malicious code on the GPU. This flaw allows a local user to crash the system or escalate their privileges on the system.
CVE-2022-0330	perf-3.10.0-1160.59.1.el7.x86_64	perf	A random memory access flaw was found in the Linux kernel's GPU i915 kernel driver functionality in the way a user may run malicious code on the GPU. This flaw allows a local user to crash the system or escalate their privileges on the system.
CVE-2021-4155	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	• 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.
CVE-2021-4155	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	• 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.
CVE-2021-4155	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	• 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.
CVE-2021-4155	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	• 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.
CVE-2021-4155	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	• 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.
CVE-2021-4155	perf-3.10.0-1160.59.1.el7.x86_64	perf	• 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.
CVE-2021-29154	kernel-3.10.0-1160.59.1.el7.x86_64	kernel	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.

CVE-2021-29154	kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel	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.
CVE-2021-29154	kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers	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.
CVE-2021-29154	kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools	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.
CVE-2021-29154	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs	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.
CVE-2021-29154	perf-3.10.0-1160.59.1.el7.x86_64	perf	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.
CVE-2021-31535	libX11-1.6.7-4.el7_9.x86_64	libX11	LookupCol.c in X.Org X through X11R7.7 and libX11 before 1.7.1 might allow remote attackers to execute arbitrary code. The libX11 XLookupColor request (intended for server-side color lookup) contains a flaw allowing a client to send color-name requests with a name longer than the maximum size allowed by the protocol (and also longer than the maximum packet size for normal-sized packets). The user-controlled data exceeding the maximum size is then interpreted by the server as additional X protocol requests and executed, e.g., to disable X server authorization completely. For example, if the victim encounters malicious terminal control sequences for color codes, then the attacker may be able to take full control of the running graphical session.
CVE-2021-31535	libX11-common-1.6.7-4.el7_9.noarch	libX11-common	LookupCol.c in X.Org X through X11R7.7 and libX11 before 1.7.1 might allow remote attackers to execute arbitrary code. The libX11 XLookupColor request (intended for server-side color lookup) contains a flaw allowing a client to send color-name requests with a name longer than the maximum size allowed by the protocol (and also longer than the maximum packet size for normal-sized packets). The user-controlled data exceeding the maximum size is then interpreted by the server as additional X protocol requests and executed, e.g., to disable X server authorization completely. For example, if the victim encounters malicious terminal control sequences for color codes, then the attacker may be able to take full control of the running graphical session.
CVE-2016-4658	libxml2-2.9.1-6.el7_9.6.x86_64	libxml2	xpointer.c in libxml2 before 2.9.5 (as used in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3, and other products) does not forbid namespace nodes in XPointer ranges, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and memory corruption) via a crafted XML document.
CVE-2016-4658	libxml2-python-2.9.1-6.el7_9.6.x86_64	libxml2-python	xpointer.c in libxml2 before 2.9.5 (as used in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3, and other products) does not forbid namespace nodes in XPointer ranges, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and memory corruption) via a crafted XML document.
CVE-2020-25717	libwbclient-4.10.16-18.el7_9.x86_64	libwbclient	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.
CVE-2020-25717	samba-4.10.16-18.el7_9.x86_64	samba	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.
CVE-2020-25717	samba-client-libs-4.10.16-18.el7_9.x86_64	samba-client-libs	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.
CVE-2020-25717	samba-common-4.10.16-18.el7_9.noarch	samba-common	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.

CVE-2020-25717	samba-common-libs-4.10.16-18.el7_9.x86_64	samba-common-libs	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.
CVE-2020-25717	samba-common-tools-4.10.16-18.el7_9.x86_64	samba-common-tools	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.
CVE-2020-25717	samba-libs-4.10.16-18.el7_9.x86_64	samba-libs	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.
CVE-2020-25717	samba-winbind-4.10.16-18.el7_9.x86_64	samba-winbind	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.
CVE-2020-25717	samba-winbind-clients-4.10.16-18.el7_9.x86_64	samba-winbind-clients	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.
CVE-2020-25717	samba-winbind-modules-4.10.16-18.el7_9.x86_64	samba-winbind-modules	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.
CVE-2016-2124	libwbclient-4.10.16-18.el7_9.x86_64	libwbclient	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2016-2124	samba-4.10.16-18.el7_9.x86_64	samba	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2016-2124	samba-client-libs-4.10.16-18.el7_9.x86_64	samba-client-libs	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2016-2124	samba-common-4.10.16-18.el7_9.noarch	samba-common	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2016-2124	samba-common-libs-4.10.16-18.el7_9.x86_64	samba-common-libs	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.

CVE-2016-2124	samba-common-tools-4.10.16-18.el7_9.x86_64	samba-common-tools	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2016-2124	samba-libs-4.10.16-18.el7_9.x86_64	samba-libs	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2016-2124	samba-winbind-4.10.16-18.el7_9.x86_64	samba-winbind	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2016-2124	samba-winbind-clients-4.10.16-18.el7_9.x86_64	samba-winbind-clients	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2016-2124	samba-winbind-modules-4.10.16-18.el7_9.x86_64	samba-winbind-modules	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2021-44142	libwbclient-4.10.16-18.el7_9.x86_64	libwbclient	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.
CVE-2021-44142	samba-4.10.16-18.el7_9.x86_64	samba	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.
CVE-2021-44142	samba-client-libs-4.10.16-18.el7_9.x86_64	samba-client-libs	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.
CVE-2021-44142	samba-common-4.10.16-18.el7_9.noarch	samba-common	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.
CVE-2021-44142	samba-common-libs-4.10.16-18.el7_9.x86_64	samba-common-libs	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.
CVE-2021-44142	samba-common-tools-4.10.16-18.el7_9.x86_64	samba-common-tools	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.

CVE-2021-44142	samba-libs-4.10.16-18.el7_9.x86_64	samba-libs	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.
CVE-2021-44142	samba-winbind-4.10.16-18.el7_9.x86_64	samba-winbind	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.
CVE-2021-44142	samba-winbind-clients-4.10.16-18.el7_9.x86_64	samba-winbind-clients	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.
CVE-2021-44142	samba-winbind-modules-4.10.16-18.el7_9.x86_64	samba-winbind-modules	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.
CVE-2021-43527	nss-3.67.0-4.el7_9.x86_64	nss	NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR are vulnerable to a heap overflow when handling DER-encoded DSA or RSA-PSS signatures. Applications using NSS for handling signatures encoded within CMS, S/MIME, PKCS #7, or PKCS #12 are likely to be impacted. Applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality may be impacted, depending on how they configure NSS. **Note: This vulnerability does NOT impact Mozilla Firefox.** However, email clients and PDF viewers that use NSS for signature verification, such as Thunderbird, LibreOffice, Evolution and Evince are believed to be impacted. This vulnerability affects NSS < 3.73 and NSS < 3.68.1.
CVE-2021-43527	nss-sysinit-3.67.0-4.el7_9.x86_64	nss-sysinit	NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR are vulnerable to a heap overflow when handling DER-encoded DSA or RSA-PSS signatures. Applications using NSS for handling signatures encoded within CMS, S/MIME, PKCS #7, or PKCS #12 are likely to be impacted. Applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality may be impacted, depending on how they configure NSS. **Note: This vulnerability does NOT impact Mozilla Firefox.** However, email clients and PDF viewers that use NSS for signature verification, such as Thunderbird, LibreOffice, Evolution and Evince are believed to be impacted. This vulnerability affects NSS < 3.73 and NSS < 3.68.1.
CVE-2021-43527	nss-tools-3.67.0-4.el7_9.x86_64	nss-tools	NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR are vulnerable to a heap overflow when handling DER-encoded DSA or RSA-PSS signatures. Applications using NSS for handling signatures encoded within CMS, S/MIME, PKCS #7, or PKCS #12 are likely to be impacted. Applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality may be impacted, depending on how they configure NSS. **Note: This vulnerability does NOT impact Mozilla Firefox.** However, email clients and PDF viewers that use NSS for signature verification, such as Thunderbird, LibreOffice, Evolution and Evince are believed to be impacted. This vulnerability affects NSS < 3.73 and NSS < 3.68.1.
CVE-2021-4034	polkit-0.112-26.el7_9.1.x86_64	polkit	A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.

Packages Updated NOT for Security Reasons

Old Package	New Package NOT for CVE
aide-0.15.1-13.el7.x86_64	aide-0.15.1-13.el7_9.1.x86_64
expat-2.1.0-12.el7.x86_64	expat-2.1.0-14.el7_9.x86_64
java-1.8.0-openjdk-headless-1.8.0.292.b10-1.el7_9.x86_64	java-1.8.0-openjdk-headless-1.8.0.312.b07-1.el7_9.x86_64
kernel-3.10.0-1160.31.1.el7.x86_64	kernel-3.10.0-1160.59.1.el7.x86_64
kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel-3.10.0-1160.59.1.el7.x86_64
kernel-headers-3.10.0-1160.31.1.el7.x86_64	kernel-headers-3.10.0-1160.59.1.el7.x86_64
kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools-3.10.0-1160.59.1.el7.x86_64
kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64
libX11-1.6.7-3.el7_9.x86_64	libX11-1.6.7-4.el7_9.x86_64
libX11-common-1.6.7-3.el7_9.noarch	libX11-common-1.6.7-4.el7_9.noarch
libwbclient-4.10.16-15.el7_9.x86_64	libwbclient-4.10.16-18.el7_9.x86_64

libxml2-2.9.1-6.el7.5.x86_64	libxml2-2.9.1-6.el7_9.6.x86_64
libxml2-python-2.9.1-6.el7.5.x86_64	libxml2-python-2.9.1-6.el7_9.6.x86_64
nspr-4.25.0-2.el7_9.x86_64	nspr-4.32.0-1.el7_9.x86_64
nss-3.53.1-3.el7_9.x86_64	nss-3.67.0-4.el7_9.x86_64
nss-softokn-3.53.1-6.el7_9.x86_64	nss-softokn-3.67.0-3.el7_9.x86_64
nss-softokn-freebl-3.53.1-6.el7_9.x86_64	nss-softokn-freebl-3.67.0-3.el7_9.x86_64
nss-sysinit-3.53.1-3.el7_9.x86_64	nss-sysinit-3.67.0-4.el7_9.x86_64
nss-tools-3.53.1-3.el7_9.x86_64	nss-tools-3.67.0-4.el7_9.x86_64
nss-util-3.53.1-1.el7_9.x86_64	nss-util-3.67.0-1.el7_9.x86_64
perf-3.10.0-1160.31.1.el7.x86_64	perf-3.10.0-1160.59.1.el7.x86_64
polkit-0.112-26.el7.x86_64	polkit-0.112-26.el7_9.1.x86_64
postgresql13-13.2-1PGDG.rhel7.x86_64	postgresql13-13.6-1PGDG.rhel7.x86_64
postgresql13-contrib-13.2-1PGDG.rhel7.x86_64	postgresql13-contrib-13.6-1PGDG.rhel7.x86_64
postgresql13-libs-13.2-1PGDG.rhel7.x86_64	postgresql13-libs-13.6-1PGDG.rhel7.x86_64
postgresql13-llvmjit-13.2-1PGDG.rhel7.x86_64	postgresql13-llvmjit-13.6-1PGDG.rhel7.x86_64
postgresql13-plpython3-13.2-1PGDG.rhel7.x86_64	postgresql13-plpython3-13.6-1PGDG.rhel7.x86_64
postgresql13-server-13.2-1PGDG.rhel7.x86_64	postgresql13-server-13.6-1PGDG.rhel7.x86_64
rawio-4.3.0.0-30699.x86_64	rawio-4.5.0.0-36989.x86_64
samba-4.10.16-15.el7_9.x86_64	samba-4.10.16-18.el7_9.x86_64
samba-client-libs-4.10.16-15.el7_9.x86_64	samba-client-libs-4.10.16-18.el7_9.x86_64
samba-common-4.10.16-15.el7_9.noarch	samba-common-4.10.16-18.el7_9.noarch
samba-common-libs-4.10.16-15.el7_9.x86_64	samba-common-libs-4.10.16-18.el7_9.x86_64
samba-common-tools-4.10.16-15.el7_9.x86_64	samba-common-tools-4.10.16-18.el7_9.x86_64
samba-libs-4.10.16-15.el7_9.x86_64	samba-libs-4.10.16-18.el7_9.x86_64
samba-winbind-4.10.16-15.el7_9.x86_64	samba-winbind-4.10.16-18.el7_9.x86_64
samba-winbind-clients-4.10.16-15.el7_9.x86_64	samba-winbind-clients-4.10.16-18.el7_9.x86_64
samba-winbind-modules-4.10.16-15.el7_9.x86_64	samba-winbind-modules-4.10.16-18.el7_9.x86_64
tzdata-java-2021a-1.el7.noarch	tzdata-java-2021c-1.el7.noarch
virt-what-1.18-4.el7.x86_64	virt-what-1.21-3.x86_64

Old Package	New Package NOT for CVE
esi-release-4.3.0.0-35578.6185.x86_64	esi-release-4.4.0.0-36479.25.x86_64
logbase-ui-4.3.0.0-20210908174753.x86_64	logbase-ui-4.4.0.0-20220113210713.x86_64
lumeta-api-4.3.0.0-35571.x86_64	lumeta-api-4.4.0.0-36477.x86_64
lumeta-api-client-4.3.0.0-35517.x86_64	lumeta-api-client-4.4.0.0-36002.x86_64
lumeta-cisco-ise-pxgrid-4.3.0.0-31455.x86_64	lumeta-cisco-ise-pxgrid-4.4.0.0-31455.x86_64
lumeta-console-4.3.0.0-35437.x86_64	lumeta-console-4.4.0.0-36225.x86_64
lumeta-diagnostics-4.3.0.0-35301.x86_64	lumeta-diagnostics-4.4.0.0-35301.x86_64
lumeta-discovery-agent-4.3.0.0-35569.x86_64	lumeta-discovery-agent-4.4.0.0-36247.x86_64
lumeta-dxl-4.3.0.0-34658.x86_64	lumeta-dxl-4.4.0.0-34658.x86_64
lumeta-install-4.3.0.0-35577.x86_64	lumeta-install-4.4.0.0-36339.x86_64

lumeta-ips-import-4.3.0.0-30740.x86_64	lumeta-ips-import-4.4.0.0-36334.x86_64
lumeta-ireg-4.3.0.0-6550.x86_64	lumeta-ireg-4.4.0.0-6550.x86_64
lumeta-lib-4.3.0.0-35480.x86_64	lumeta-lib-4.4.0.0-36203.x86_64
lumeta-pam-4.3.0.0-34789.x86_64	lumeta-pam-4.4.0.0-34789.x86_64
lumeta-tools-4.3.0.0-34180.x86_64	lumeta-tools-4.4.0.0-35385.x86_64
lumeta-ui-4.3.0.0-35247.x86_64	lumeta-ui-4.4.0.0-36238.x86_64
lumeta-visio-4.3.0.0-34789.x86_64	lumeta-visio-4.4.0.0-34789.x86_64
lumeta-warehouse-4.3.0.0-35421.x86_64	lumeta-warehouse-4.4.0.0-36429.x86_64
lumeta-webapp-4.3.0.0-35385.x86_64	lumeta-webapp-4.4.0.0-35919.x86_64

New Packages

New Packages
lumeta-api-python-4.5.0.0-36740.x86_64

Removed Packages

Removed Packages
postgresql-libs-9.2.24-1.el7_5.x86_64