Pkg	Affected versions	Vulnerability	Links
zstd	1.4.10-1.5.4	Supplying empty string as a command argument causes buffer overrun.	CVE-2022-4899
zlib1g(-dev)		MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_64 via a long filename, comment, or extra field. NOTE: MiniZip is not a supported part of the zlib product. NOTE: pyminizip through 0.2.6 is also vulnerable because it bundles an affected zlib version, and exposes the applicable MiniZip code through its compress API.	CVE-2023-45853
zip	3.0	Info-ZIP Zip 3.0, when the -T and -TT command-line options are used, allows attackers to cause a denial of service (invalid free and application crash) or possibly have unspecified other impact because of an off-by-one error. NOTE: it is unclear whether there are realistic scenarios in which an untrusted party controls the -TT value, given that the entire purpose of -TT is execution of arbitrary commands	CVE-2018-13410
xz-utils	5.2.5	Attackers can cause DoS via decompression of a crafted file. Claims of "endless output"/"DoS" disputed: decompression of the 17,486 bytes always results in 114,881,179 bytes, not an unreasonable size increase.	CVE-2020-22916 security.snyk.io
xserver-xorg-video-nouveau	Ubuntu 18.04-24.04, Nouveau NV117	A remote DoS vulnerability exists in the way Nouveau handles GPU shader execution. A specially crafted pixel shader can cause remote DoS issues. Attackers can provide specially crafted websites to trigger this.	CVE-2018-3979
xrdp	< 0.9.21	• Out of Bound Write in xrdp_mm_trans_process_drdynvc_channel_open() • Buffer over flow in xrdp_login_wnd_create(), audin_send_open(), devredir_proc_client_devlist_announce_req(), xrdp_mm_chan_data_in(), • Out of Bound Read in xrdp_caps_process_confirm_active(), xrdp_mm_trans_process_drdynvc_channel_close(), xrdp_sec_process_mcs_data_CS_CORE(), libxrdp_send_to_channel() • Integer Overflow in xrdp_mm_process_rail_update_window_text()	CVE-2022-23478 CVE-2022-23468 CVE-2022-23477 CVE-2022-23479 CVE-2022-23481 CVE-2022-23493 CVE-2022-23482 CVE-2022-23483 CVE-2022-23484

	< 0.9.23	auth_start_session() can return non-zero (1) value on, e.g., PAM error which may result in in session restrictions such as max concurrent sessions per user by PAM (ex ./etc/security/limits.conf) to be bypassed. Users (administrators) don't use restrictions by PAM are not affected.	CVE-2023-40184
	< 0.9.23.1	Access to the font glyphs in xrdp_painter.c is not bounds-checked . Since some of this data is controllable by the user, this can result in an out-of-bounds read within the xrdp executable. The vulnerability allows an out-of-bounds read within a potentially privileged process. On non-Debian platforms, xrdp tends to run as root. Potentially an out-of-bounds write can follow the out-of-bounds read. There is no denial-of-service impact, providing xrdp is running in forking mode.	CVE-2023-42822
xorg has a lower version, why? xserver-common, xserver-xorg-core e.g. have an unaffected version. CVEs belong to “xorg-server”	< 2:21.1.4-2ubuntu1.7~22.04.10		CVE-2024-31083
	< 2:21.1.4-2ubuntu1.7~22.04.9		CVE-2024-31081 CVE-2024-31080 CVE-2024-31082
	< 2:21.1.4-2ubuntu1.7~22.04.7		CVE-2024-21885 CVE-2024-0229 CVE-2024-0408 CVE-2023-6816 CVE-2024-21886 CVE-2024-0409
	< 2:21.1.4-2ubuntu1.7~22.04.5		CVE-2023-6478 CVE-2023-6377
	< 2:21.1.4-2ubuntu1.7~22.04.2		CVE-2023-5367 CVE-2023-5380

	< 2:21.1.3-2ubuntu2.7		CVE-2023-0494
	< 2:21.1.3-2ubuntu2.5		CVE-2022-4283 CVE-2022-46342 CVE-2022-46343 CVE-2022-46344 CVE-2022-46341 CVE-2022-46340
	< 2:21.1.3-2ubuntu2.3		CVE-2022-3550 CVE-2022-3551
	< 2:21.1.3-2ubuntu2.1		CVE-2022-2319 CVE-2022-2320
	< 2:1.20.13-1ubuntu2		CVE-2021-4011 CVE-2021-4008 CVE-2021-4009 CVE-2021-4010
	< 2:1.20.11-1ubuntu1		CVE-2021-3472
	< 2:1.16.2.901-1ubuntu4		CVE-2015-0255
xdg-utils	*	When xdg-mail is configured to use thunderbird for mailto URLs, improper parsing of the URL can lead to additional headers being passed to thunderbird that should not be included per RFC 2368. An attacker can use this method to create a mailto URL that looks safe to users, but will actually attach files when clicked.	CVE-2022-4055

x11vnc (no exact match in package list)		Not yet analyzed by NVD.	CVE-2019-15690
wget	*	Does not omit Authorization header upon redirect to different origin, related to CVE-2018-1000007.	CVE-2021-31879
vim	< 2:8.2.3995-1ubuntu2.9		CVE-2022-0696 CVE-2022-0393 CVE-2022-0407 CVE-2022-0158 CVE-2022-0156 CVE-2022-0128
	< 2:8.2.3995-1ubuntu2.8		CVE-2023-2609 CVE-2023-2610 CVE-2023-2426
	< 2:8.2.3995-1ubuntu2.7		CVE-2022-2207 CVE-2022-0729 CVE-2022-0714 CVE-2022-0685 CVE-2022-0629 CVE-2022-0572 CVE-2022-0554

			CVE-2022-0443 CVE-2022-0408 CVE-2022-0359 CVE-2022-0351 CVE-2022-0361 CVE-2022-0368 CVE-2022-0261 CVE-2022-0319 CVE-2022-0213 CVE-2022-0318
	< 2:8.2.3995-1ubuntu2.5		CVE-2022-2980 CVE-2022-2946 CVE-2022-2923 CVE-2022-2849 CVE-2022-2845 CVE-2022-2581 CVE-2022-2571 CVE-2022-2344 CVE-2022-2345

			CVE-2022-2206 CVE-2022-2304 CVE-2022-2175 CVE-2022-2129 CVE-2022-2126 CVE-2022-2124 CVE-2022-2125 CVE-2022-1968 CVE-2022-1942 CVE-2022-1927 CVE-2022-1898 CVE-2022-1851 CVE-2022-1796 CVE-2022-1785 CVE-2022-1735 CVE-2022-1733 CVE-2022-1720 CVE-2022-1674 CVE-2022-1629

			CVE-2022-0413
	< 2:8.2.3995-1ubuntu2.4		CVE-2023-1264 CVE-2023-1175 CVE-2023-1170 CVE-2022-47024 CVE-2023-0433 CVE-2023-0288 CVE-2023-0054 CVE-2023-0051 CVE-2023-0049
	< 2:8.2.3995-1ubuntu2.3		CVE-2022-0417 CVE-2022-0392
util-linux	(may be patched)		CVE-2024-28085
unzip			CVE-2021-4217
ubuntu-drivers-common	*	Removed from the official package manager, contains malicious code. Attempts to impersonate a valid organization, but no connection between that organization and the package's authorship.	CWE-506
tnftp	*		CVE-2014-8517
telnet	*	Buffer overflow in the handle_packet function in mactelnet.c in the client in MAC-Telnet 0.4.3 and earlier allows remote TELNET servers to execute arbitrary code via a long string in an MT_CPTYPE_PASSSALT control packet.	CVE-2016-7115
tcpdump (may be useful, captures		The ppp decapsulator in tcpdump 4.9.3 can be convinced to allocate a large amount of memory.	CVE-2020-8037

network traffic!)			
tar	< 1.34+dfsg-1.2ubuntu 1.1		CVE-2023-398 04 CVE-2019-992 3
systemd	*	systemd-resolved may accept records of DNSSEC-signed domains even when they have no signature, allowing man-in-the-middles (or the upstream DNS resolver) to manipulate records.	CVE-2023-700 8
	< 249.11-0ubuntu3.7	• Can cause a local information leak due to systemd-coredump not respecting the fs.suid_dumpable kernel setting. • Off-by-one Error in format_timespan() of time-util.c. An attacker could supply specific values for time and accuracy that leads to buffer overrun in format_timespan(), leading to DoS.	CVE-2022-441 5 CVE-2022-382 1
sudo	< 1.9.13p1-1ubuntu2	does not escape control characters in sudoreplay output and log messages.	CVE-2023-284 87 CVE-2023-284 86
squashfs-tool s	Description says 4.5 vulnerable, snyk.io says fixed in 4.4.	squashfs_opendir in unsquash-2.c in Squashfs-Tools 4.5 allows Directory Traversal. A squashfs filesystem that has been crafted to include a symbolic link and then contents under the same filename in a filesystem can cause unsquashfs to first create the symbolic link pointing outside the expected directory, and then the subsequent write operation will cause the unsquashfs process to write through the symbolic link elsewhere in the filesystem.	CVE-2021-410 72
		squashfs_opendir in unsquash-1.c in Squashfs-Tools 4.5 stores the filename in the directory entry; this is then used by unsquashfs to create the new file during the unsquash. The filename is not validated for traversal outside of the destination directory, and thus allows writing to locations outside of the destination.	CVE-2021-401 53
snapd	*	An issue in the Unmarshal function in Go-Yaml v3 causes the program to crash when attempting to deserialize invalid input.	CVE-2022-289 48
slirp4netns	<4.3.1	Out-of-bounds read vulnerability in the SLiRP networking implementation of the QEMU emulator. Occurs in icmp6_send_echoreply() while replying to an ICMP echo request. Allows attackers to leak the contents of the host memory, resulting in information disclosure.	CVE-2020-107 56
rsyslog	<8.22.04.1, may be fixed in ubuntu's 8.2112.0)	Heap-based Buffer Overflow when octet-counted framing is used. Attacker can corrupt heap values, leading to data integrity issues and availability impact. Note: If users do not need octet-counted, they can turn it off for the most important modules.	CVE-2022-249 03

	<8.27.0	Integer Overflow or Wraparound. A DoS vulnerability was found in rsyslog in the imptcp module. An attacker could send a specially crafted message to the imptcp socket, which would cause rsyslog to crash.	CVE-2018-16881
python3, python3.10 (has a lower versions, but CVE's belong to package python3.10. Package python3 affected too?)	*	The email module of Python through 3.11.3 incorrectly parses e-mail addresses that contain a special character. The wrong portion of an RFC2822 header is identified as the value of the addr-spec. In some applications, an attacker can bypass a protection mechanism in which application access is granted only after verifying receipt of e-mail to a specific domain (e.g., only @company.example.com addresses may be used for signup). This occurs in email/_parseaddr.py in recent versions of Python.	CVE-2023-27043
	<3.10.12-1~22.04.3	Affects servers (e.g., HTTP) that use TLS client authentication. If a TLS server-side socket is created, receives data into the socket buffer, and then is closed quickly, there is a brief window where the SSLSocket instance will detect the socket as "not connected" and won't initiate a handshake, but buffered data will still be readable from the socket buffer. This data will not be authenticated if the server-side TLS peer is expecting client certificate authentication, and is indistinguishable from valid TLS stream data. Data is limited in size to the amount that will fit in the buffer. (The TLS connection cannot directly be used for data exfiltration because the vulnerable code path requires that the connection be closed on initialization of the SSLSocket.)	CVE-2023-40217
	<3.10.12-1~22.04.2	Directory traversal vulnerability in the (1) extract and (2) extractall functions in the tarfile module in Python allows user-assisted remote attackers to overwrite arbitrary files via a .. (dot dot) sequence in filenames in a TAR archive, a related issue to CVE-2001-1267.	CVE-2007-4559
	<3.10.6-1~22.04.2ubuntu1.1	An issue in the urllib.parse component of Python before 3.11.4 allows attackers to bypass blocklisting methods by supplying a URL that starts with blank characters.	CVE-2023-24329
		An unnecessary quadratic algorithm exists in one path when processing some inputs to the IDNA (RFC 3490) decoder, such that a crafted, unreasonably long name being presented to the decoder could lead to a CPU denial of service. Hostnames are often supplied by remote servers that could be controlled by a malicious actor; in such a scenario, they could trigger excessive CPU consumption on the client attempting to make use of an attacker-supplied supposed hostname. For example, the attack payload could be placed in the Location header of an HTTP response with status code 302. A fix is planned in 3.11.1, 3.10.9, 3.9.16, 3.8.16, and 3.7.16.	CVE-2022-45061
		The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties. This occurs in the sponge function interface.	CVE-2022-37454
	<3.10.6-1~22.04.1	allows local privilege escalation in a non-default configuration. The Python multiprocessing library, when used with the forkserver start method on Linux, allows pickles to be deserialized from any user in the same machine local network	CVE-2022-42919

		namespace, which in many system configurations means any user on the same machine. Pickles can execute arbitrary code. Thus, this allows for local user privilege escalation to the user that any forkserver process is running as. Setting multiprocessing.util.abstract_sockets_supported to False is a workaround. The forkserver start method for multiprocessing is not the default start method.	
		Open redirection vulnerability in lib/http/server.py due to no protection against multiple (/) at the beginning of URI path which may leads to information disclosure.	CVE-2021-28861
python3-twisted	<23.10.0rc1, may be fixed in 22.1.0-2ubuntu2.4	when sending multiple HTTP requests in one TCP packet, twisted.web will process the requests asynchronously without guaranteeing the response order. If one of the endpoints is controlled by an attacker, the attacker can delay the response on purpose to manipulate the response of the second request when a victim launched two requests using HTTP pipeline	CVE-2023-46137
	<22.10.0rc1, may be fixed in 22.1.0-2ubuntu2.4	Started with version 0.9.4, when the host header does not match a configured host twisted.web.vhost.NameVirtualHost will return a NoResource resource which renders the Host header unescaped into the 404 response allowing HTML and script injection. In practice this should be very difficult to exploit as being able to modify the Host header of a normal HTTP request implies that one is already in a privileged position.	CVE-2022-39348
python3-zope	<5.8.6		CVE-2023-44389
	<5.8.5		CVE-2023-42458
python3-systemd	<249.11-0ubuntu3.7	• Local information leak due to systemd-coredump not respecting the fs.suid_dumpable kernel setting. • Off-by-one Error in format_timespan() of time-util.c. An attacker could supply specific values for time and accuracy that leads to buffer overrun, leading to DoS.	CVE-2022-4415 CVE-2022-3821
	<248.3-1ubuntu3	basic/unit-name.c has a Memory Allocation with an Excessive Size Value (involving strdupa and alloca for a pathname controlled by a local attacker), resulting in an OS crash.	CVE-2021-33910
		DoS. A specially crafted DHCP FORCERENEW packet can cause a server running the DHCP client to be vulnerable to a DHCP ACK spoofing attack. An attacker can forge a pair of FORCERENEW and DCHP ACK packets to reconfigure the server.	CVE-2020-13529
	<244.1-0ubuntu3	Heap use-after-free vulnerability, where asynchronous Polkit queries are performed while handling dbus messages. A local unprivileged attacker can abuse this flaw to crash systemd services or potentially execute code and elevate their privileges, by sending specially crafted dbus messages.	CVE-2020-1712

python3-setuptools	<65.5.1, may be fixed in 59.6.0-1.2ubuntu0.22.04.1	Python Packaging Authority (PyPA) setuptools allows remote attackers to cause a DoS via HTML in a crafted package or custom PackageIndex page. There is a Regular Expression DoS (ReDoS) in package_index.py.	CVE-2022-40897
python3-openssl	>22.0.0?		CVE-2024-2511
	*	Uses typosquatting to bait unknowing users to install them. It installs malware in user's system that leaks their data.	security.snyk.io
python3-oauthlib	<3.2.2, may be fixed in 3.2.0-1ubuntu0.1	An attacker providing malicious redirect URI can cause DoS. An attacker can also leverage usage of uri_validate functions depending where it is used. OAuthLib applications using OAuth2.0 provider support or use directly uri_validate are affected by this issue. Version 3.2.1 contains a patch. There are no known workarounds.	CVE-2022-36087
gnome-keyring (perhaps python3 too?)	*	Allows local users to retrieve login credentials via a Secret Service API call and the D-Bus interface if the keyring is unlocked, a similar issue to CVE-2008-7320. One perspective is that this occurs because available D-Bus protection mechanisms (involving the busconfig and policy XML elements) are not used.	CVE-2018-19358
python3-jwt	<2.4.0	Vulnerable to Use of a Broken or Risky Cryptographic Algorithm via non-blacklisted public key formats, leading to key confusion.	CVE-2022-29217
	<3.3.4	Vulnerable to Authentication Bypass. An attacker who obtains a JWT can arbitrarily forge its contents without knowing the secret key. Depending on the application, this may for example enable the attacker to spoof other user's identities, hijack their sessions, or bypass authentication.	security.snyk.io
python3-idna	<3.7	Vulnerable to Resource Exhaustion via the idna.encode function. An attacker can consume significant resources and potentially cause a DoS by supplying specially crafted arguments to this function.	CVE-2024-3651
dbus (python3 too?)	*	Sometimes allows unprivileged users to crash dbus-daemon. If a privileged user with control over the dbus-daemon is using the org.freedesktop.DBus.Monitoring interface to monitor message bus traffic, then an unprivileged user with the ability to connect to the same dbus-daemon can cause a dbus-daemon crash under some circumstances via an unreplyable message. When done on the well-known system bus, this is a denial-of-service vulnerability. The fixed versions are 1.12.28, 1.14.8, and 1.15.6.	CVE-2023-34969
	<1.12.24 <1.12.20-2ubuntu4.1	An authenticated attacker can cause dbus-daemon and other programs that use libdbus to crash when receiving a message with certain invalid type signatures or with array length inconsistent with element type size, or sending a message with attached file descriptors in an unexpected format.	CVE-2022-42010 CVE-2022-42012 CVE-2022-42011

python3-cryptography	May be fixed in 3.4.8-1ubuntu2.2	May allow a remote attacker to decrypt captured messages in TLS servers that use RSA key exchanges	CVE-2023-50782
python3-configobj	*	Regular Expression DoS (ReDoS) via the validate function, using (.+?)((.*)). Only exploitable in the case of a developer putting the offending value in a server side configuration file.	CVE-2023-26112
apport (python3 too?)	*		CVE-2022-28653
	<2.21.0-0ubuntu1		CVE-2021-3899
procps	>=3.3.0	Allows a user who has access to run the “ps” utility to write unlimited unfiltered data into the process heap.	CVE-2023-4016
policykit-1	*	pkexec, when used with --user nonpriv, allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.	CVE-2016-2568
perl	May be fixed in 5.34.0-3ubuntu1.3	function S_find_uninit_var in sv.c has a stack-based crash that can lead to remote code execution or local privilege escalation.	CVE-2022-48522
patch	>=2.7	Invalid Pointer vulnerability via the another_hunk function, which causes a DoS, and double free.	CVE-2021-45261 CVE-2018-6952
openssl	[3.0.0, 3.0.13[, may be fixed in 3.0.2-0ubuntu1.14	Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow, ...	CVE-2023-5678 CVE-2024-0727 CVE-2023-6237 CVE-2023-6129
openssh	<9.6, may befixed in 1:8.9p1-3ubuntu0.6	OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.	CVE-2023-51385
		In sh-agent, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.	CVE-2023-51384

	<9.3, may be fixed in 1:8.9p1-3ubuntu0.3/0.5	PKCS#11 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009. ssh-add adds smartcard keys to ssh-agent without the intended per-hop destination constraints.	CVE-2023-38408 CVE-2023-28531
ntfs-3g	<2022.10.3, may be fixed in 1:2021.8.22-3ubuntu1.2	Buffer overflow. Crafted metadata in an NTFS image can cause code execution. A local attacker can exploit this if the ntfs-3g binary is setuid root. A physically proximate attacker can exploit this if NTFS-3G is configured to execute upon attachment of an external storage device.	CVE-2022-40284
	<=2021.8.22, may be fixed in 3ubuntu1.1	Invalid return code in fuse_kern_mount enables intercepting of libfuse-lite protocol traffic between NTFS-3G and the kernel.	CVE-2022-30783
		A crafted NTFS image can cause heap exhaustion in ntfs_get_attribute_value, or a heap-based buffer overflow in ntfs_names_full_collate, ntfs_mft_rec_alloc and ntfs_check_log_client_array.	CVE-2022-30784 CVE-2022-30786 CVE-2022-30788 CVE-2022-30789
		A file handle created in fuse_lib_opendir, and later used in fuse_lib_readdir, enables arbitrary memory read and write operations when using libfuse-lite.	CVE-2022-30785
		Integer underflow in fuse_lib_readdir enables arbitrary memory read operations in NTFS-3G through 2021.8.22 when using libfuse-lite.	CVE-2022-30787
needrestart	<3.6, may be fixed in 3.5-5ubuntu2.1	Prone to local privilege escalation. Regexes to detect the Perl, Python, and Ruby interpreters are not anchored, allowing a local user to escalate privileges when needrestart tries to detect if interpreters are using old source files.	CVE-2022-30688
ncurses	*	NULL pointer dereference in tgetstr in tinfo/lib_termcap.c.	CVE-2023-45918
		Segmentation fault via the component _nc_wrap_entry().	CVE-2023-50495
	<6.4, may be fixed in 6.3-2ubuntu0.1	When used by a setuid application, allows local users to trigger security-relevant memory corruption via malformed data in a terminfo database file that is found in $HOME/.terminfo or reached via the TERMINFO or TERM environment variable.	CVE-2023-29491
multipath-tools	<0.9.2, may be fixed in 0.8.8-1ubuntu1.22.04.1	Allows local users to obtain root access. Local users able to access /dev/shm can change symlinks in multipathd due to incorrect symlink handling, which could lead to controlled file writes outside of the /dev/shm directory. This could be used indirectly for local privilege escalation to root. Also, Local users able to write to UNIX domain sockets can bypass access controls and manipulate the multipath setup. This can lead	CVE-2022-41973 CVE-2022-41974

		to local privilege escalation to root. This occurs because an attacker can repeat a keyword, which is mishandled because arithmetic ADD is used instead of bitwise OR.	
mdadm	<4.2-rc2	Buffer overflow in some Intel(R) SSD Tools software may allow a privileged user to potentially enable escalation of privilege via local access.	CVE-2023-28736
		Uncontrolled resource consumption in some Intel(R) SSD Tools software may allow a priviledged user to potentially enable DoS via local access.	CVE-2023-28938
logrotate	<3.20.0, may be fixed in 3.19.0-1ubuntu1.1	When the state file does not exist, it is created with world-readable permission, allowing an unprivileged user to lock the state file, stopping any rotation.	CVE-2022-1348
libzstd	1.4.1-1.4.9, may be fixed in dfsg-2build1	zstd creates output files with default permissions and restricts them immediately afterwards. Output files could thus momentarily be readable or writable to attackers.	CVE-2021-24032 security.snyk.io
libyaml	<0.2.5	Affected is the function yaml_emitter_emit_flow_sequence_item in /src/libyaml/src/emitter.c. The manipulation leads to heap-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259052.	CVE-2024-3205
libXpm	<0:3.5.13-10.el9, may be fixed in 1:3.5.12-1ubuntu0.22.04.2	boundary condition within the XpmCreateXpmImageFromBuffer() function. This flaw allows a local attacker to trigger an out-of-bounds read error and read the contents of memory on the system.	CVE-2023-43788 CVE-2023-43789
	<=3.5.15, may be fixed in 1:3.5.12-1ubuntu0.22.04.1	When processing files with .Z or .gz extensions, the library calls external programs to compress and uncompress files, relying on the PATH environment variable to find these programs, which could allow a malicious user to execute other programs by manipulating the PATH environment variable.	CVE-2022-4883
		issue when parsing a file with a comment not closed; the end-of-file condition will not be detected, leading to an infinite loop and resulting in a DoS in the application linked to the library.	CVE-2022-46285
		When processing a file with width of 0 and a very large height, some parser functions will be called repeatedly and can lead to an infinite loop, resulting in a Denial of Service in the application linked to the library.	CVE-2022-44617
libxml2	<2.11.7, may be fixed in 2.9.13+dfsg-1ubuntu0.4	When using the XML Reader interface with DTD validation and XInclude expansion enabled, processing crafted XML documents can lead to an xmlValidatePopElement use-after-free.	CVE-2024-25062
	<2.10.4, may be fixed in	When hashing empty dict strings in a crafted XML document, xmlDictComputeFastKey in dict.c can produce non-deterministic values, leading to various logic and memory	CVE-2023-29469

	2.9.13+dfsg-1ubuntu 0.3	errors, such as a double free. This behavior occurs because there is an attempt to use the first byte of an empty string, and any value is possible (not solely the '\0' value). Parsing of certain invalid XSD schemas can lead to a NULL pointer dereference and subsequently a segfault. This occurs in xmlSchemaFixupComplexType in xmlschemas.c.	CVE-2023-28484
	<2.10.3, may be fixed in 2.9.13+dfsg-1ubuntu 0.2	Certain invalid XML entity definitions can corrupt a hash table key, potentially leading to subsequent logic errors. In one case, a double-free can be provoked. When parsing a multi-gigabyte XML document with the XML_PARSE_HUGE parser option enabled, several integer counters can overflow. This results in an attempt to access an array at a negative 2GB offset, typically leading to a segmentation fault.	CVE-2022-40304 CVE-2022-40303
	<2.9.14, may be fixed in 2.9.13+dfsg-1ubuntu 0.2/0.1	NULL Pointer Dereference allows attackers to cause DoS. Allows triggering crashes through forged input data, given a vulnerable code sequence in the application. The vulnerability is caused by the iterwalk function (also used by the canonicalize function). Such code shouldn't be in wide-spread use, given that parsing + iterwalk would usually be replaced with the more efficient iterparse function. However, an XML converter that serialises to C14N would also be vulnerable, for example, and there are legitimate use cases for this code sequence. If untrusted input is received (also remotely) and processed via iterwalk function, a crash can be triggered. Several buffer handling functions in buf.c (xmlBuf*) and tree.c (xmlBuffer*) don't check for integer overflows. This can result in out-of-bounds memory writes. Exploitation requires a victim to open a crafted, multi-gigabyte XML file. Other software using libxml2's buffer functions, for example libxslt through 1.1.35, is affected as well.	CVE-2022-2309 CVE-2022-29824
libxml-twig-perl	*	The option to expand_external_ents, documented as controlling external entity expansion in XML::Twig does not work. External entities are always expanded, regardless of the option's setting.	CVE-2016-9180
libx11	May be fixed in 2:1.7.5-1ubuntu0.3	Integer overflow in XCreateImage(), allows a local user to trigger an integer overflow and execute arbitrary code with elevated privileges.	CVE-2023-43787
		Infinite loop in PutSubImage(). Allows DoS.	CVE-2023-43786
		Boundary condition in _XkbReadKeySyms(). Allows a local user to trigger an out-of-bounds read error and read the contents of memory on the system.	CVE-2023-43785
	<=libX11 1.8.6, may be fixed in 2:1.7.5-1ubuntu0.2	Functions in src/InitExt.c in libX11 do not check that the values provided for the Request, Event, or Error IDs are within the bounds of the arrays that those functions write to, using those IDs as array indexes. They trust that they were called with values provided by an Xserver adhering to the bounds specified in the X11 protocol, as all X servers provided by X.Org do. As the protocol only specifies a single byte for these values, an out-of-bounds value provided by a malicious server (or a malicious proxy-in-the-middle) can only overwrite other portions of the Display structure and not	CVE-2023-3138

		write outside the bounds of the Display structure itself, possibly causing the client to crash with this memory corruption.	
libwebp	<1.3.2, may be fixed in 1.2.2-2ubuntu0.22.04.2	Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)	CVE-2023-4863
	<1.3.1, may be fixed in 1.2.2-2ubuntu0.22.04.1	Use after free/double free in libwebp. An attacker can use the ApplyFiltersAndEncode() function and loop through to free best.bw and assign best = trial pointer. The second loop will then return 0 because of an Out of memory error in VP8 encoder, the pointer is still assigned to trial and the AddressSanitizer will attempt a double free.	CVE-2023-1999
libuv1	<1.48.0, may be fixed in 1.43.0-1ubuntu0.1	Server-Side Request Forgery (SSRF)	CVE-2024-24806
libtirpc3	<1.3.3rc1, may be fixed in 1.3.2-2ubuntu0.1	Remote attackers could exhaust the file descriptors of a process that uses libtirpc because idle TCP connections are mishandled. This can, in turn, lead to an svc_run infinite loop without accepting new connections.	CVE-2021-46828
libssh (vulnerable pkg #60)	<0:0.10.4-13.el9, may be fixed in 0.9.6-2ubuntu0.22.04.3		CVE-2023-6004
			CVE-2023-6918 CVE-2023-48795 CVE-2023-48795 CVE-2023-2283 CVE-2023-1667 CVE-2021-3634
librsvg	<2.56.3, may be fixed in 2.52.5+dfsg-3ubuntu0.2	A directory traversal problem in the URL decoder of librsvg before 2.56.3 could be used by local or remote attackers to disclose files (on the local filesystem outside of the expected area), as demonstrated by href="?../../../../../../../../../../etc/passwd" in an xi:include element.	CVE-2023-38633
libpng	*	A crafted PNG image can lead to a segmentation fault and denial of service in png_setup_paeth_row() function.	CVE-2022-3857

CVE-2023-20593		Security framework issue that may allow unauthorized access through misconfigured profiles.	x
CVE-2023-50471		Local privilege escalation vulnerability in Linux kernel allowing users to gain elevated privileges.	apparmor 3.0.4-2 x
Apport 2.20.11		Vulnerability in the Linux kernel permitting unauthorized local privilege escalation.	https://www.exploit-db.com/exploits/49572 x Tried with exploit 1
APT 2.4.12		Local privilege escalation in Ubuntu affecting polkit; exploited via manipulated environment variables.	https://www.exploit-db.com/exploits/46676 x
CVE-2021-3493		Multiple BIND vulnerabilities affecting DNS services; can lead to denial-of-service attacks.	https://github.com/JlSakuya/Linux-Privilege-Escalation-Exploits/tree/main/2021/CVE-2021-3493 x Tried with exploit 2
Bind9-utils		Security notice detailing vulnerabilities in various packages; critical for system integrity.	https://www.cloudfoundry.org/blog/usn-6633-1-bind-vulnerabilities/
Binutils		Buffer overflow in the Linux kernel that could allow local privilege escalation.	https://ubuntu.com/security/notices/USN-6544-1
Bolt		Vulnerability allowing elevation of privileges due to improper validation in certain Linux modules.	https://www.exploit-db.com/exploits/48296 x

containerd.io		Various security issues reported; specific vulnerabilities can lead to privilege escalation.	CVE-2024-21626 x
cpio 2.13		Requires physical access to exploit disk encryption weaknesses, risking data exposure.	packetstormsecurity x Tried with exploit4
Cryptsetup		Vulnerability affecting EULER OS; may lead to privilege escalation or denial of service.	https://linuxiac.com/cryptsetup-vulnerability/ Physical access required
Dmidecode		Security vulnerabilities in E2fsprogs project; affects filesystem utilities and potential local privilege escalation.	https://vulners.com/nessus/EULEROS_SA-2023-2720.NASL
E2fsprogs		Security notice for vulnerabilities in Ubuntu packages, critical for maintaining system security.	https://www.cvedetails.com/vulnerability-list/vendor_id-15251/E2fsprogs-Project.html
Fdisk		Overview of local privilege escalation vulnerabilities in the Linux kernel with available exploits.	https://vulners.com/nessus/UBUNTU_USN-6719-1.NASL
Finalrd		Kernel vulnerability allowing local users to escalate privileges via improper validation.	https://juggernaut-sec.com/kernel-exploits-lpe/ x
Findutils		Security guide detailing FTP vulnerabilities, emphasizing exploitation methods.	CVE-2007-2452
ftp		Vulnerability in a Linux service leading to local privilege escalation through improper handling.	https://book.hacktricks.xyz/network-services-pentesting/pentesting-ftp

Fuse3		Security flaw that allows unauthorized access to sensitive data in a specific software environment.	https://www.exploit-db.com/exploits/45106 x
Gawk		Critical security notice detailing vulnerabilities in Ubuntu affecting system integrity.	https://vulners.com/veracode/VERACODE:42878 x
Polkit		Vulnerability in Git affecting Ubuntu 22.04, posing a risk of unauthorized access.	https://vulners.com/ubuntu/USN-4980-1 x
Git		Insight into GRUB vulnerabilities affecting system booting, which can lead to arbitrary code execution.	https://security.snyk.io/vuln/SNYK-UBUNTU2204-GIT-3051753 x
Grub		Buffer overflow vulnerability in a popular Linux application allowing local privilege escalation.	https://medium.com/ssd-secure-disclosure/bothole-a-look-at-gnu-grub-vulnerabilities-d15c66effe60 x
Info		Local privilege escalation vulnerability found in specific Linux services or applications.	https://www.exploit-db.com/exploits/34030 x
Init		Exploration of vulnerabilities in Intel's microcode, affecting system security and stability.	CVE-2023-39415
Intel-microcode		Security vulnerabilities related to iptables configurations that could lead to unauthorized access.	https://hackaday.com/2022/07/19/down-the-intel-microcode-rabbit-hole/

IPTables		Vulnerability in a popular service leading to potential local privilege escalation.	https://vulmon.com/searchpage?q=iptables
IPUTILS-ping		Security issue in Linux systems allowing unauthorized users to gain elevated privileges.	https://www.exploit-db.com/exploits/9688 x
Iputils-tracepath		Exploitable flaw in a system service that may allow for privilege escalation.	https://www.exploit-db.com/exploits/178 x
Irqbabalance		Vulnerability allowing remote code execution in ISC DHCP server configurations.	https://www.exploit-db.com/exploits/15823 x
Isc-dhcp-common		Resource detailing local privilege escalation vulnerabilities and their mitigation strategies.	https://vulners.com/nessus/ISC_DHCP_CVE-2019-6470.NASL
Kmod		Notice on critical vulnerabilities in Ubuntu packages that require immediate attention.	https://www.win.tue.nl/~aeb/linux/hh/hh-12.html x
Kpartx		Vulnerability in CentOS that could lead to unauthorized access or denial of service.	https://vulners.com/ubuntu/USN-5731-1
Less		A privilege escalation vulnerability affecting Linux systems, allowing unauthorized elevation of privileges.	https://vulners.com/nessus/CENTOS9_LESS-590-2.NASL
lib32stdc++		Local privilege escalation vulnerability in certain Linux components due to improper checks.	CVE-2023-4039

Libacl1		Repeated reference to the same privilege escalation vulnerability in Linux systems.	https://www.exploit-db.com/exploits/48818
Libatomic1		Overview of internal read gadgets in Python leading to potential data exposure vulnerabilities.	CVE-2023-4039
Libattr1		Resource on payloads used in privilege escalation attacks within Linux environments.	https://book.hacktricks.xyz/generic-methodologies-and-resources/python/python-internal-read-gadgets
Libaudit		Vulnerability report detailing potential exploit scenarios affecting system security.	https://book.hacktricks.xyz/linux-hardening/privilege-escalation/payloads-to-execute
Libavahi		Local privilege escalation vulnerability in a commonly used Linux application.	https://www.tenable.com/plugins/nessus/151452
Libbinutils		Security notice regarding vulnerabilities in libbpf, critical for maintaining system security.	https://www.exploit-db.com/exploits/42386
Libbpf		Vulnerability in a service that may allow local privilege escalation through improper handling.	https://www.cloudfoundry.org/blog/usn-5759-1-libbpf-vulnerabilities/
LIbbz2		Security flaw in a popular application leading to potential data leaks or unauthorized access.	https://www.exploit-db.com/exploits/18147

Libc		Security notice addressing vulnerabilities in Ubuntu, critical for system integrity.	CVE-2023-4911
Libclang 1:14.0.0		**USN-5464-1**: A vulnerability in Ubuntu affecting packages that could allow a local user to gain elevated privileges.	https://vulners.com/nessus/UBUNTU_USN-6258-1.NASL
Licom-err2		**UBUNTU_USN-6361-1**: A vulnerability affecting a component of Ubuntu that allows local users to execute arbitrary code.	https://vulners.com/ubuntu/USN-5464-1
Libcups			https://vulners.com/nessus/UBUNTU_USN-6361-1.NASL
Libcurl		**curl 7.81.0**: A flaw in Curl that could lead to a denial of service due to improper handling of certain inputs.	https://curl.se/docs/vuln-7.81.0.html
Libdb5.3		**CVE-2019-8457**: Windows GDI vulnerability that allows an attacker to execute arbitrary code via a crafted application.	CVE-2019-8457
Libdbus		**Exploit-21323**: A vulnerability that enables local users to escalate privileges by exploiting a flaw in the software.	https://www.exploit-db.com/exploits/21323
Libdconf		**Exploit-42276**: A vulnerability related to privilege escalation in a common application that allows attackers to gain unauthorized access.	https://www.exploit-db.com/exploits/42276
Libefl1		**CVE-2021-3711**: OpenSSL vulnerability in RSA key generation that may result in weak keys, compromising security.	CVE-2021-3711

Libestr0		**CPE-Detail**: Details regarding software versions and configurations that could lead to vulnerabilities.	https://nvd.nist.gov/products/cpe/detail/B98B6DD5-435B-4F3E-AABE-A86649F75BCA?namingFormat=2.3&orderBy=CPEURI&keyword=cpe%3A2.3%3Aa%3Aadiscon&status=FINAL%2CDEPRECATED
Libevent-core		**Nessus Plugin 97721**: A vulnerability identified by Nessus that highlights a security issue in specific software.	https://www.tenable.com/plugins/nessus/97721
Libevent		**CVE-2023-52425**: A vulnerability in a PGP plugin for WordPress allowing arbitrary PHP code execution.	https://www.tenable.com/plugins/nessus/97721
Libexpat			CVE-2023-52425
Libfakeroot		**The Dangerous of Fakeroot**: A discussion about vulnerabilities associated with the Fakeroot tool that could lead to security issues.	https://full-disclosure.grok.org.narkive.com/nY2zIaET/the-dangerous-of-fakeroot
Libfile		**Exploit-51331**: A known vulnerability that enables attackers to exploit a software flaw for malicious purposes.	https://www.exploit-db.com/exploits/51331
Libfridi		**USN-5922-1**: A vulnerability notice related to certain Ubuntu packages that could be exploited by local users.	https://vulners.com/ubuntu/USN-5922-1

Libgcab		**Nessus Plugin 106348**: A Nessus vulnerability report indicating a security issue in specific packages.	https://www.tenable.com/plugins/nessus/106348
Libgcc		**Snyk Vulnerability**: A security flaw in a library that may expose applications to attacks.	https://security.snyk.io/vuln/SNYK-AMZN2023-LIBGCC-5893950
Libgcrypt		**USN-5080-1**: An Ubuntu security notice concerning a vulnerability that allows privilege escalation.	https://vulners.com/nessus/UBUNTU_USN-5080-1.NASL
Libgdbm		**Exploit-38049**: A specific vulnerability exploit documented in the Exploit Database.	https://www.exploit-db.com/exploits/38049
Libgif		**Snyk Vulnerability LIBGIF7**: A security vulnerability in the GIF processing library that could allow exploitation.	https://security.snyk.io/vuln/SNYK-SLES152-LIBGIF7-5458984
LibG		**Nessus Plugin 195216**: A security vulnerability report identified by Nessus affecting certain software.	https://www.tenable.com/plugins/nessus/195216
LibGL1		**Exploit-20127**: A vulnerability in a common application that can lead to exploitation.	https://www.exploit-db.com/exploits/20127
Glib		**USN-4764-1**: An Ubuntu security notice indicating vulnerabilities in certain software packages.	https://vulners.com/ubuntu/USN-4764-1
GStreamer		**Exploit-42162**: A documented vulnerability that allows unauthorized access or control over a system.	https://www.exploit-db.com/exploits/42162

LibICE		**REDHAT_UNPATCHED**: A notice regarding unpatched vulnerabilities in specific Red Hat components.	https://vulners.com/nessus/REDHAT_UNPATCHED-LIBICE-RHEL6.NASL
LibIP		**Exploit-50808**: A vulnerability that allows privilege escalation in software applications.	https://www.exploit-db.com/exploits/50808
LibISL		**Exploit-51737**: An exploit that targets a vulnerability in a specific application or system.	https://www.exploit-db.com/exploits/51737
Libisns		**ld.so.conf-example**: A document discussing privilege escalation techniques related to shared libraries.	https://book.hacktricks.xyz/linux-hardening/privilege-escalation/ld.so.conf-example
Libgig		**Exploit-42546**: A vulnerability exploit for specific applications leading to potential unauthorized access.	https://www.exploit-db.com/exploits/42546
JSON token exploit for RStudio server		**JSON Serialization Exploit**: An article discussing security vulnerabilities associated with improper JSON serialization.	https://medium.com/@s12deff/exploit-json-serialization-e617a75f6663
KLibc		**USN-6736-1**: An Ubuntu security notice related to vulnerabilities in specific components.	https://vulners.com/ubuntu/USN-6736-1
Libkrb		**Nessus Plugin 184451**: A security vulnerability affecting specific software components identified by Nessus.	https://www.tenable.com/plugins/nessus/184451
Libksba		**Snyk Vulnerability LIBKSBA**: A vulnerability in a library that could lead to security issues in applications.	https://security.snyk.io/vuln/SNYK-ORACLE8-LIBKSBA-3062863

Lapack		**Nessus Plugin 196553**: Another vulnerability report from Nessus highlighting security issues.	https://www.tenable.com/plugins/nessus/196553
OpenLDAP		**Nessus Plugin 189773**: A vulnerability report from Nessus affecting specific packages.	https://www.tenable.com/plugins/nessus/189773
LibMLN		**CVE-2023-0179 PoC**: Proof of Concept for a local privilege escalation vulnerability in the Linux kernel.	https://github.com/TurtleARM/CVE-2023-0179-PoC
SnapD		**Exploit-46362**: An exploit targeting a known vulnerability in certain applications.	https://www.exploit-db.com/exploits/46362
Libnetplan		**CVE-2023-4039**: A vulnerability in Ubuntu's libc-bin that allows local users to gain root privileges.	https://ubuntu.com/security/CVE-2023-4039
LibNettle		**USN-4990-1**: An Ubuntu security notice indicating vulnerabilities that need to be addressed.	https://vulners.com/ubuntu/USN-4990-1
Libnftnl			https://github.com/TurtleARM/CVE-2023-0179-PoC/blob/master/exploit.c
Libnsl-dev			https://hackaday.com/2024/03/29/security-alert-potential-ssh-backdoor-via-liblzma/
Libntfs		**CVE-2019-9755**: A vulnerability in lzma extraction functionality allowing remote denial of service.	CVE-2019-9755

Libpam		1. **Exploit-50963**: A specific vulnerability exploit documented in the Exploit Database.	https://www.exploit-db.com/exploits/50963

Found no CVEs for: zerofree, xxd, xkb-data, libxkbcommon, xinput, xinit, xfsprog, xfonts, xcvt, xbitmaps, xauth, libx11, x11, wireless-regdb, whiptail, uuid, usrmerge, usbutils, usbmuxd, usb.ids, usb-modeswitch, upower, update-notifier, update-manager, unattended-upgrades, ufw, udisks, udev, ucf, ubuntu-standard, ubuntu-* (except drivers-common), tzdata, tpm-udev, tmux, time, tilix, thin-provisioning-tools, thermald, sysvinit, strace (monitors interactions with the linux kernel), ssl-cert, ssh-import-id, squashfs, strace, ssl-cert, ssh-import-id, sosreport, software-properties-common, sntp, snap, share-mime-info, sg3-utils(-udev), session-migration, sensible-utils, sed, secureboot-db, scrot, screen, sbsigntool, run-one, rsync, rstudio-server, rpcsvc-proto, readline-common, r-*, python3-[minimal, zipp, yaml, xkit, wadllib, update-manager, software-properties, six, service-identity, serial, secretstorage, pyparsing, pyasn1, ptyprocess, problem-report, pkg-resources, pexpect, newt, netifaces, magic, lib2to3, lazr, launchpadlib, jeepney, incremental, importlib, hyperlink, httplib2, hamcrest, gi, gdbm, dist*, debian, debconf, constantly, commandnotfound, colorama, click, chardet, cffi, blinker, bcrypt, automat, attr, apt, apport], publicsuffix, psmisc, powermgmt, pollinate, polkitd, Plymouth, pkg-config, pkexec, pinentry, pigz, pciutils, pci.ids, pastebinit, passwd, parted, packagekit, overlayroot, os-prober, openbox, open-vm-tools, open-iscsi, obconf, ntp, nftables, network-dispatcher, netplan, netfilter, netcat, netbase, nano, mtr, mount, motd, modemmanager, mime-support, mesa-vulkan, media-types, mawk, manpages, man-db, make, mailcap, lynx, lxd, lvm2, lto-disabled-list, lsof, lshw, lsb, logsave, login, locales, linux-*, libxxhash, libxxf86, libxvmc, libxv, libxtst, libxtables, libxt, libxss, libxshmfence, libxrender, libxrandr, libxmuu, libxmu, libxmlsec, libxmlb, libxml-xpathengine, libxml-parser, libxkbfile, libxkbcommon, libxinerama, libxi, libxft, libxfont, libxfixes, libxext, libxdmcp, libxdamage, libxcvt, libxcursor, libxcomposite, libxcb*, libxaw, libxau, libxatracker, libx11-*, libwww, libwrap, libwayland, libvulkan, libvted, libvte, libvolume, libuuid, libutempter, libusbmuxd, libusb, liburi, liburcu, libupower, libunwind, libunistring, libudisks, libudev, libuchardet, libubsan, libtss2-*, libtsan, libtry, libtk, libtinfo, libtimedate, libtiff5, libtie, libthai, libtext, libterm, libtcl, libtasn, libsystemd, libstemmer, libstdc, libstartup, libssl, libss2, libsqlite, libsort, libsodium, libsmbios, libsmartcol, libsm6, libslirp, libslang, libsigsegv, libsgutils, libsepol, libsensors, libsemanage, libseccomp, libsasl, librtmp, libreadline, libquadmath, libqmi, libpython3, libpsl, libprocps, libproc, libpq, libpopt, libpolkit, libplymouth, libplist, libpixman, libpipeline, libphobos, libperl, libpciaccess.