Security Export

SCA scan: DONE, Wed Jun 5, 2024

Contextual Analysis scan: NOT_SCANNED, Wed Jun 5, 2024

Exported on: Fri Jun 7, 2024

Exported by: rn185124@ncr.com

Package type: Docker

Sha256: c13374cc83121ec5ced961e019ba078bb6a9e8744fd44e6d1474ad849ea76f4c

Component name: launchpad:1.21.0-3023-PR.769

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Due to a failure in validating the number of scanline samples of a OpenEXR file containing deep scanline data, Academy Software Foundation OpenEXÂ image parsing library version 3.2.1 and prior is susceptible to a heap-based buffer overflow vulnerability. This issue was resolved as of versionsÂ v3.2.2 and v3.1.12 of the affected library.	CVE-2023-5841	Critical	High		debian:bookworm:libopenexr-3-1-30	All Versions		0001-01-01T00:00:00Z	Not Covered
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	Critical	High		debian:bookworm:zlib1g	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Increasing the resolution of video frames, while performing a multi-threaded encode, can result in a heap overflow in av1_loop_restoration_dealloc().	CVE-2023-6879	Critical	Low		debian:bookworm:libaom3	All Versions		0001-01-01T00:00:00Z	Not Covered
An out of bounds read exists in libjxl. An attacker using a specifically crafted file could cause an out of bounds read in the exif handler. We recommend upgrading to version 0.8.1 or past commitÂ https://github.com/libjxl/libjxl/pull/2101/commits/d95b050c1822a5b1ede9e0dc937e43fca1b10159 https://github.com/libjxl/libjxl/pull/2101/commits/d95b050c1822a5b1ede9e0dc937e43fca1b10159	CVE-2023-0645	Critical			debian:bookworm:libjxl0.7	All Versions		0001-01-01T00:00:00Z	Not Covered
Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.	CVE-2023-50387	High	High		debian:bookworm:libpam-systemd	All Versions		0001-01-01T00:00:00Z	Not Covered
Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.	CVE-2023-50387	High	High		debian:bookworm:libsystemd-shared	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.	CVE-2023-50387	High	High		debian:bookworm:libsystemd0	All Versions		0001-01-01T00:00:00Z	Not Covered
Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.	CVE-2023-50387	High	High		debian:bookworm:libudev1	All Versions		0001-01-01T00:00:00Z	Not Covered
Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.	CVE-2023-50387	High	High		debian:bookworm:systemd-sysv	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.	CVE-2023-50387	High	High		debian:bookworm:systemd	All Versions		0001-01-01T00:00:00Z	Not Covered
Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.	CVE-2023-50387	High	High		debian:bookworm:libnss-systemd	All Versions		0001-01-01T00:00:00Z	Not Covered
Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.	CVE-2023-50387	High	High		debian:bookworm:systemd-timesyncd	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.	CVE-2023-50387	High	High		debian:bookworm:udev	All Versions		0001-01-01T00:00:00Z	Not Covered
libexpat through 2.5.0 allows a denial of service (resource consumption) because many full reparsings are required in the case of a large token for which multiple buffer fills are needed.	CVE-2023-52425	High	High		debian:bookworm:libexpat1	All Versions		0001-01-01T00:00:00Z	Not Covered
In GNOME GdkPixbuf (aka gdk-pixbuf) through 2.42.10, the ANI (Windows animated cursor) decoder encounters heap memory corruption (in ani_load_chunk in io-ani.c) when parsing chunks in a crafted .ani file. A crafted file could allow an attacker to overwrite heap metadata, leading to a denial of service or code execution attack. This occurs in gdk_pixbuf_set_option() in gdk-pixbuf.c.	CVE-2022-48622	High	High		debian:bookworm:libgdk-pixbuf2.0-bin	All Versions		0001-01-01T00:00:00Z	Not Covered
In GNOME GdkPixbuf (aka gdk-pixbuf) through 2.42.10, the ANI (Windows animated cursor) decoder encounters heap memory corruption (in ani_load_chunk in io-ani.c) when parsing chunks in a crafted .ani file. A crafted file could allow an attacker to overwrite heap metadata, leading to a denial of service or code execution attack. This occurs in gdk_pixbuf_set_option() in gdk-pixbuf.c.	CVE-2022-48622	High	High		debian:bookworm:libgdk-pixbuf2.0-common	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
In GNOME GdkPixbuf (aka gdk-pixbuf) through 2.42.10, the ANI (Windows animated cursor) decoder encounters heap memory corruption (in ani_load_chunk in io-ani.c) when parsing chunks in a crafted .ani file. A crafted file could allow an attacker to overwrite heap metadata, leading to a denial of service or code execution attack. This occurs in gdk_pixbuf_set_option() in gdk-pixbuf.c.	CVE-2022-48622	High	High		debian:bookworm:libgdk-pixbuf-2.0-0	All Versions		0001-01-01T00:00:00Z	Not Covered
CPAN.pm before 2.35 does not verify TLS certificates when downloading distributions over HTTPS.	CVE-2023-31484	High	High		debian:bookworm:libperl5.36	All Versions		0001-01-01T00:00:00Z	Not Covered
CPAN.pm before 2.35 does not verify TLS certificates when downloading distributions over HTTPS.	CVE-2023-31484	High	High		debian:bookworm:perl-base	All Versions		0001-01-01T00:00:00Z	Not Covered
CPAN.pm before 2.35 does not verify TLS certificates when downloading distributions over HTTPS.	CVE-2023-31484	High	High		debian:bookworm:perl	All Versions		0001-01-01T00:00:00Z	Not Covered
CPAN.pm before 2.35 does not verify TLS certificates when downloading distributions over HTTPS.	CVE-2023-31484	High	High		debian:bookworm:perl-modules-5.36	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.12.5. 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	High	Medium		debian:bookworm:libxml2	All Versions		0001-01-01T00:00:00Z	Not Covered
A segment fault (SEGV) flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFReadRGBATileExt() API. This flaw allows a remote attacker to cause a heap-buffer overflow, leading to a denial of service.	CVE-2023-52356	High	Medium		debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
An out-of-memory flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFRasterScanlineSize64() API. This flaw allows a remote attacker to cause a denial of service via a crafted input with a size smaller than 379 KB.	CVE-2023-52355	High	Medium		debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An unchecked return value in TLS handshake code could have caused a potentially exploitable crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.9, and Thunderbird < 115.9.	CVE-2024-0743	High	Medium		debian:bookworm:libnss3	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in SQLite SQLite3 up to 3.43.0 and classified as critical. This issue affects the function sessionReadRecord of the file ext/session/sqlite3session.c of the component make alltest Handler. The manipulation leads to heap-based buffer overflow. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-248999.	CVE-2023-7104	High	Medium		debian:bookworm:libsqlite3-0	All Versions		0001-01-01T00:00:00Z	Not Covered
libheif v1.17.5 was discovered to contain a segmentation violation via the function UncompressedImageCodec::get_luma_bits_per_pixel_from_configuration_unci.	CVE-2023-49464	High	Medium		debian:bookworm:libheif1	All Versions		0001-01-01T00:00:00Z	Not Covered
libheif v1.17.5 was discovered to contain a segmentation violation via the function find_exif_tag at /libheif/exif.cc.	CVE-2023-49463	High	Medium		debian:bookworm:libheif1	All Versions		0001-01-01T00:00:00Z	Not Covered
libheif v1.17.5 was discovered to contain a segmentation violation via the component /libheif/exif.cc.	CVE-2023-49462	High	Medium		debian:bookworm:libheif1	All Versions		0001-01-01T00:00:00Z	Not Covered
libheif v1.17.5 was discovered to contain a segmentation violation via the function UncompressedImageCodec::decode_uncompressed_image.	CVE-2023-49460	High	Medium		debian:bookworm:libheif1	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in Python 3.11 through 3.11.4. If a path containing '\0' bytes is passed to os.path.normpath(), the path will be truncated unexpectedly at the first '\0' byte. There are plausible cases in which an application would have rejected a filename for security reasons in Python 3.10.x or earlier, but that filename is no longer rejected in Python 3.11.x.	CVE-2023-41105	High	Medium	sha256__adaa6238f46912e8d63b00b1f48b33d7a2a256ca20f094421876c2203e342b67.tar.gz/usr/bin/python3.11	python:python	3.11.0a1 <= Version <= 3.12.0rc1		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in Python 3.11 through 3.11.4. If a path containing '\0' bytes is passed to os.path.normpath(), the path will be truncated unexpectedly at the first '\0' byte. There are plausible cases in which an application would have rejected a filename for security reasons in Python 3.10.x or earlier, but that filename is no longer rejected in Python 3.11.x.	CVE-2023-41105	High	Medium		debian:bookworm:libpython3.11-stdlib	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in Python 3.11 through 3.11.4. If a path containing '\0' bytes is passed to os.path.normpath(), the path will be truncated unexpectedly at the first '\0' byte. There are plausible cases in which an application would have rejected a filename for security reasons in Python 3.10.x or earlier, but that filename is no longer rejected in Python 3.11.x.	CVE-2023-41105	High	Medium		debian:bookworm:python3.11	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in Python 3.11 through 3.11.4. If a path containing '\0' bytes is passed to os.path.normpath(), the path will be truncated unexpectedly at the first '\0' byte. There are plausible cases in which an application would have rejected a filename for security reasons in Python 3.10.x or earlier, but that filename is no longer rejected in Python 3.11.x.	CVE-2023-41105	High	Medium		debian:bookworm:python3.11-minimal	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in Python 3.11 through 3.11.4. If a path containing '\0' bytes is passed to os.path.normpath(), the path will be truncated unexpectedly at the first '\0' byte. There are plausible cases in which an application would have rejected a filename for security reasons in Python 3.10.x or earlier, but that filename is no longer rejected in Python 3.11.x.	CVE-2023-41105	High	Medium		debian:bookworm:libpython3.11-minimal	All Versions		0001-01-01T00:00:00Z	Not Covered
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	High	Medium		debian:bookworm:libpython3.11-stdlib	All Versions		2023-03-19T08:11:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
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	High	Medium		debian:bookworm:python3.11-minimal	All Versions		2023-03-19T08:11:00Z	Not Covered
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	High	Medium		debian:bookworm:libpython3.11-minimal	All Versions		2023-03-19T08:11:00Z	Not Covered
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	High	Medium		debian:bookworm:python3.11	All Versions		2023-03-19T08:11:00Z	Not Covered
hb-ot-layout-gsubgpos.hh in HarfBuzz through 6.0.0 allows attackers to trigger O(n^2) growth via consecutive marks during the process of looking back for base glyphs when attaching marks.	CVE-2023-25193	High	Medium		debian:bookworm:libharfbuzz-icu0	All Versions		2023-03-19T08:23:00Z	Not Covered
hb-ot-layout-gsubgpos.hh in HarfBuzz through 6.0.0 allows attackers to trigger O(n^2) growth via consecutive marks during the process of looking back for base glyphs when attaching marks.	CVE-2023-25193	High	Medium		debian:bookworm:libharfbuzz0b	All Versions		2023-03-19T08:23:00Z	Not Covered
AOMedia v3.0.0 to v3.5.0 was discovered to contain an invalid read memory access via the component assign_frame_buffer_p in av1/common/av1_common_int.h.	CVE-2023-39616	High	Low		debian:bookworm:libaom3	All Versions		0001-01-01T00:00:00Z	Not Covered
Integer Overflow vulnerability in Mbed TLS 2.x before 2.28.7 and 3.x before 3.5.2, allows attackers to cause a denial of service (DoS) via mbedtls_x509_set_extension().	CVE-2024-23775	High			debian:bookworm:libmbedcrypto7	All Versions		0001-01-01T00:00:00Z	Not Covered
cJSON v1.7.16 was discovered to contain a segmentation violation via the function cJSON_InsertItemInArray at cJSON.c.	CVE-2023-50471	High			debian:bookworm:libcjson1	All Versions		0001-01-01T00:00:00Z	Not Covered
Multiple signed integers overflow in function au_read_header in src/au.c and in functions mat4_open and mat4_read_header in src/mat4.c in Libsndfile, allows an attacker to cause Denial of Service or other unspecified impacts.	CVE-2022-33065	High			debian:bookworm:libsndfile1	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An off-by-one error in function wav_read_header in src/wav.c in Libsndfile 1.1.0, results in a write out of bound, which allows an attacker to execute arbitrary code, Denial of Service or other unspecified impacts.	CVE-2022-33064	High			debian:bookworm:libsndfile1	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in dec_patch_dictionary.cc in libjxl before 0.8.2. An integer underflow in patch decoding can lead to a denial of service, such as an infinite loop.	CVE-2023-35790	High			debian:bookworm:libjxl0.7	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in openldap. This security flaw causes a null pointer dereference in ber_memalloc_x() function.	CVE-2023-2953	High			debian:bookworm:libldap-2.5-0	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in openldap. This security flaw causes a null pointer dereference in ber_memalloc_x() function.	CVE-2023-2953	High			debian:bookworm:libldap-common	All Versions		0001-01-01T00:00:00Z	Not Covered
Dmidecode before 3.5 allows -dump-bin to overwrite a local file. This has security relevance because, for example, execution of Dmidecode via Sudo is plausible.	CVE-2023-30630	High			debian:bookworm:dmidecode	All Versions		0001-01-01T00:00:00Z	Not Covered
A heap-based buffer overflow was found in openjpeg in color.c:379:42 in sycc420_to_rgb when decompressing a crafted .j2k file. An attacker could use this to execute arbitrary code with the permissions of the application compiled against openjpeg.	CVE-2021-3575	High			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An attacker may cause an HTTP/2 endpoint to read arbitrary amounts of header data by sending an excessive number of CONTINUATION frames. Maintaining HPACK state requires parsing and processing all HEADERS and CONTINUATION frames on a connection. When a request's headers exceed MaxHeaderBytes, no memory is allocated to store the excess headers, but they are still parsed. This permits an attacker to cause an HTTP/2 endpoint to read arbitrary amounts of header data, all associated with a request which is going to be rejected. These headers can include Huffman-encoded data which is significantly more expensive for the receiver to decode than for an attacker to send. The fix sets a limit on the amount of excess header frames we will process before closing a connection.	CVE-2023-45288	Medium	Medium	sha256__3ec2866c9b479e30e6b72b94a5de81c4ac6a69c0c88664c51c52c265e21a7563.tar.gz/usr/local/ncr_scot/sendscox-util/sendscox/golang.org/x/net	golang.org/x/net	< 0.23.0	0.23.0	0001-01-01T00:00:00Z	Not Covered
An attacker may cause an HTTP/2 endpoint to read arbitrary amounts of header data by sending an excessive number of CONTINUATION frames. Maintaining HPACK state requires parsing and processing all HEADERS and CONTINUATION frames on a connection. When a request's headers exceed MaxHeaderBytes, no memory is allocated to store the excess headers, but they are still parsed. This permits an attacker to cause an HTTP/2 endpoint to read arbitrary amounts of header data, all associated with a request which is going to be rejected. These headers can include Huffman-encoded data which is significantly more expensive for the receiver to decode than for an attacker to send. The fix sets a limit on the amount of excess header frames we will process before closing a connection.	CVE-2023-45288	Medium	Medium	sha256__3ec2866c9b479e30e6b72b94a5de81c4ac6a69c0c88664c51c52c265e21a7563.tar.gz/usr/local/ncr_scot/sendscox-util/sendscox/github.com/golang/go	github.com/golang/go	< 1.21.9,1.22.0-0 <= Version < 1.22.2	1.21.9,1.22.2	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
loadImage() in tools/tiffcrop.c in LibTIFF through 4.5.0 has a heap-based use after free via a crafted TIFF image.	CVE-2023-26965	Medium	Medium		debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
A heap buffer overflow issue was found in ImageMagick. When an application processes a malformed TIFF file, it could lead to undefined behavior or a crash causing a denial of service.	CVE-2022-3213	Medium	Medium		debian:bookworm:imagemagick-6-common	All Versions		2023-01-08T19:25:00Z	Not Covered
A heap buffer overflow issue was found in ImageMagick. When an application processes a malformed TIFF file, it could lead to undefined behavior or a crash causing a denial of service.	CVE-2022-3213	Medium	Medium		debian:bookworm:libmagickcore-6.q16-6	All Versions		2023-01-08T19:25:00Z	Not Covered
A heap buffer overflow issue was found in ImageMagick. When an application processes a malformed TIFF file, it could lead to undefined behavior or a crash causing a denial of service.	CVE-2022-3213	Medium	Medium		debian:bookworm:libmagickwand-6.q16-6	All Versions		2023-01-08T19:25:00Z	Not Covered
A heap buffer overflow issue was found in ImageMagick. When an application processes a malformed TIFF file, it could lead to undefined behavior or a crash causing a denial of service.	CVE-2022-3213	Medium	Medium		debian:bookworm:libmagickcore-6.q16-6-extra	All Versions		2023-01-08T19:25:00Z	Not Covered
The protojson.Unmarshal function can enter an infinite loop when unmarshaling certain forms of invalid JSON. This condition can occur when unmarshaling into a message which contains a google.protobuf.Any value, or when the UnmarshalOptions.DiscardUnknown option is set.	CVE-2024-24786	Medium		sha256__3ec2866c9b479e30e6b72b94a5de81c4ac6a69c0c88664c51c52c265e21a7563.tar.gz/usr/local/ncr_scot/sendscox-util/sendscox/google.golang.org/protobuf	google.golang.org/protobuf	< 1.33.0	1.33.0	0001-01-01T00:00:00Z	Not Covered
An issue was discovered in Mbed TLS 2.x before 2.28.7 and 3.x before 3.5.2. There was a timing side channel in RSA private operations. This side channel could be sufficient for a local attacker to recover the plaintext. It requires the attacker to send a large number of messages for decryption, as described in "Everlasting ROBOT: the Marvin Attack" by Hubert Kario.	CVE-2024-23170	Medium			debian:bookworm:libmbedcrypto7	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.	CVE-2024-0727	Medium			debian:bookworm:libssl3	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.	CVE-2024-0727	Medium			debian:bookworm:openssl	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked login process) via mkfifo because the openat call (for protect_dir) lacks O_DIRECTORY.	CVE-2024-2265	Medium			debian:bookworm:libpam0g	All Versions		0001-01-01T00:00:00Z	Not Covered
linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked login process) via mkfifo because the openat call (for protect_dir) lacks O_DIRECTORY.	CVE-2024-2265	Medium			debian:bookworm:libpam-modules	All Versions		0001-01-01T00:00:00Z	Not Covered
linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked login process) via mkfifo because the openat call (for protect_dir) lacks O_DIRECTORY.	CVE-2024-2265	Medium			debian:bookworm:libpam-modules-bin	All Versions		0001-01-01T00:00:00Z	Not Covered
linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked login process) via mkfifo because the openat call (for protect_dir) lacks O_DIRECTORY.	CVE-2024-2265	Medium			debian:bookworm:libpam-runtime	All Versions		0001-01-01T00:00:00Z	Not Covered
A heap use-after-free issue has been identified in SQLite in the jsonParseAddNodeArray() function in sqlite3.c. This flaw allows a local attacker to leverage a victim to pass specially crafted malicious input to the application, potentially causing a crash and leading to a denial of service.	CVE-2024-0232	Medium			debian:bookworm:libsqlite3-0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of	CVE-2023-6129	Medium			debian:bookworm:libssl3	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used. This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue.									

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of	CVE-2023-6129	Medium			debian:bookworm:openssl	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used. This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue.									
Multiple NSS NIST curves were susceptible to a side-channel attack known as "Minerva". This attack could potentially allow an attacker to recover the private key. This vulnerability affects Firefox < 121.	CVE-2023-6135	Medium			debian:bookworm:libnss3	All Versions		0001-01-01T00:00:00Z	Not Covered
NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _nc_wrap_entry().	CVE-2023-50495	Medium			debian:bookworm:libncurses6	All Versions		0001-01-01T00:00:00Z	Not Covered
NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _nc_wrap_entry().	CVE-2023-50495	Medium			debian:bookworm:ncurses-base	All Versions		0001-01-01T00:00:00Z	Not Covered
NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _nc_wrap_entry().	CVE-2023-50495	Medium			debian:bookworm:libtinfo6	All Versions		0001-01-01T00:00:00Z	Not Covered
NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _nc_wrap_entry().	CVE-2023-50495	Medium			debian:bookworm:libncursesw6	All Versions		0001-01-01T00:00:00Z	Not Covered
NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _nc_wrap_entry().	CVE-2023-50495	Medium			debian:bookworm:ncurses-bin	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was found in CPython 3.12.0 `subprocess` module on POSIX platforms. The issue was fixed in CPython 3.12.1 and does not affect other stable releases. When using the `extra_groups=` parameter with an empty list as a value (ie `extra_groups=[]`) the logic regressed to not call `setgroups(0, NULL)` before calling `exec()`, thus not dropping the original processes' groups before starting the new process. There is no issue when the parameter isn't used or when any value is used besides an empty list. This issue only impacts CPython processes run with sufficient privilege to make the `setgroups` system call (typically `root`).	CVE-2023-6507	Medium		sha256__adaa6238f46912e8d63b00b1f48b33d7a2a256ca20f094421876c2203e342b67.tar.gz/usr/bin/python3.11	python:python	3.12.0	3.12.1	0001-01-01T00:00:00Z	Not Covered
An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may allow a remote attacker to cause a denial of service via a craft input with size smaller than 379 KB.	CVE-2023-6277	Medium			debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a	CVE-2023-5678	Medium			debian:bookworm:libssl3	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the "-pubcheck" option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.									

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a	CVE-2023-5678	Medium			debian:bookworm:openssl	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the "-pubcheck" option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.									
Artifex Software jbig2dec v0.20 was discovered to contain a SEGV vulnerability via jbig2_error at /jbig2dec/jbig2.c.	CVE-2023-46361	Medium			debian:bookworm:libjbig2dec0	All Versions		0001-01-01T00:00:00Z	Not Covered
libxml2 through 2.11.5 has a use-after-free that can only occur after a certain memory allocation fails. This occurs in xmlUnlinkNode in tree.c. NOTE: the vendor's position is "I don't think these issues are critical enough to warrant a CVE ID ... because an attacker typically can't control when memory allocations fail."	CVE-2023-45322	Medium			debian:bookworm:libxml2	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in Avahi. A reachable assertion exists in the avahi_escape_label() function.	CVE-2023-38470	Medium			debian:bookworm:libavahi-common3	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in Avahi. A reachable assertion exists in the avahi_escape_label() function.	CVE-2023-38470	Medium			debian:bookworm:libavahi-client3	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in Avahi, where a reachable assertion exists in avahi_dns_packet_append_record.	CVE-2023-38469	Medium			debian:bookworm:libavahi-common3	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A vulnerability was found in Avahi, where a reachable assertion exists in avahi_dns_packet_append_record.	CVE-2023-38469	Medium			debian:bookworm:libavahi-client3	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in Avahi. A reachable assertion exists in the avahi_alternative_host_name() function.	CVE-2023-38473	Medium			debian:bookworm:libavahi-client3	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in Avahi. A reachable assertion exists in the avahi_alternative_host_name() function.	CVE-2023-38473	Medium			debian:bookworm:libavahi-common3	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in Avahi. A reachable assertion exists in the avahi_rdata_parse() function.	CVE-2023-38472	Medium			debian:bookworm:libavahi-client3	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in Avahi. A reachable assertion exists in the avahi_rdata_parse() function.	CVE-2023-38472	Medium			debian:bookworm:libavahi-common3	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in Avahi. A reachable assertion exists in the dbus_set_host_name function.	CVE-2023-38471	Medium			debian:bookworm:libavahi-client3	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in Avahi. A reachable assertion exists in the dbus_set_host_name function.	CVE-2023-38471	Medium			debian:bookworm:libavahi-common3	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:libcc1-0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:libgfortran5	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:cpp-12	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:libtsan2	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:libatomic1	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:libitm1	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:g++-12	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:gcc-12-base	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:libsan0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:gcc-12	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:libquadmath0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:libgomp1	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:libgcc-s1	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:libstdc++6	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:libasan8	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Medium			debian:bookworm:libubsan1	All Versions		0001-01-01T00:00:00Z	Not Covered
A flaw was found in shadow-utils. When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory.	CVE-2023-4641	Medium			debian:bookworm:login	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A flaw was found in shadow-utils. When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory.	CVE-2023-4641	Medium			debian:bookworm:passwd	All Versions		0001-01-01T00:00:00Z	Not Covered
Xmlsoft Libxml2 v2.11.0 was discovered to contain an out-of-bounds read via the xmlSAX2StartElement() function at /libxml2/SAX2.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via supplying a crafted XML file. NOTE: the vendor's position is that the product does not support the legacy SAX1 interface with custom callbacks; there is a crash even without crafted input.	CVE-2023-39615	Medium			debian:bookworm:libxml2	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in Python before 3.8.18, 3.9.x before 3.9.18, 3.10.x before 3.10.13, and 3.11.x before 3.11.5. It primarily affects servers (such as HTTP servers) 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	Medium			debian:bookworm:python3.11	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in Python before 3.8.18, 3.9.x before 3.9.18, 3.10.x before 3.10.13, and 3.11.x before 3.11.5. It primarily affects servers (such as HTTP servers) 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	Medium			debian:bookworm:python3.11-minimal	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in Python before 3.8.18, 3.9.x before 3.9.18, 3.10.x before 3.10.13, and 3.11.x before 3.11.5. It primarily affects servers (such as HTTP servers) 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	Medium			debian:bookworm:libpython3.11-stdlib	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in Python before 3.8.18, 3.9.x before 3.9.18, 3.10.x before 3.10.13, and 3.11.x before 3.11.5. It primarily affects servers (such as HTTP servers) 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	Medium			debian:bookworm:libpython3.11-minimal	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered IW44EncodeCodec.cpp in djvulibre 3.5.28 in allows attackers to cause a denial of service via divide by zero.	CVE-2021-46312	Medium			debian:bookworm:libdjvulibre21	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered IW44EncodeCodec.cpp in djvulibre 3.5.28 in allows attackers to cause a denial of service via divide by zero.	CVE-2021-46312	Medium			debian:bookworm:libdjvulibre-text	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered IW44Image.cpp in djvulibre 3.5.28 in allows attackers to cause a denial of service via divide by zero.	CVE-2021-46310	Medium			debian:bookworm:libdjvulibre21	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered IW44Image.cpp in djvulibre 3.5.28 in allows attackers to cause a denial of service via divide by zero.	CVE-2021-46310	Medium			debian:bookworm:libdjvulibre-text	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability infaad2 v.2.10.1 allows a remote attacker to execute arbitrary code and cause a denial of service via the mp4info function in mp4read.c:1039.	CVE-2023-38858	Medium			debian:bookworm:libfaad2	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability infaad2 v.2.10.1 allows a remote attacker to execute arbitrary code and cause a denial of service via the stcoin function in mp4read.c.	CVE-2023-38857	Medium			debian:bookworm:libfaad2	All Versions		0001-01-01T00:00:00Z	Not Covered
A flaw was found in libtiff. A specially crafted tiff file can lead to a segmentation fault due to a buffer overflow in the Fax3Encode function in libtiff/tif_fax3.c, resulting in a denial of service.	CVE-2023-3618	Medium			debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
libtiff 4.5.0 is vulnerable to Buffer Overflow via /libtiff/tools/tiffcrop.c:8499. Incorrect updating of buffer size after rotateImage() in tiffcrop cause heap-buffer-overflow and SEGV.	CVE-2023-25433	Medium			debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
A null pointer dereference issue was found in Libtiff's tif_dir.c file. This issue may allow an attacker to pass a crafted TIFF image file to the tiffcp utility which triggers a runtime error that causes undefined behavior. This will result in an application crash, eventually leading to a denial of service.	CVE-2023-2908	Medium			debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
libtiff 4.5.0 is vulnerable to Buffer Overflow in uv_encode() when libtiff reads a corrupted little-endian TIFF file and specifies the output to be big-endian.	CVE-2023-26966	Medium			debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in the C AMQP client library (aka rabbitmq-c) through 0.13.0 for RabbitMQ. Credentials can only be entered on the command line (e.g., for amqp-publish or amqp-consume) and are thus visible to local attackers by listing a process and its arguments.	CVE-2023-35789	Medium			debian:bookworm:librabbitmq4	All Versions		0001-01-01T00:00:00Z	Not Covered
VideoLAN dav1d before 1.2.0 has a thread_task.c race condition that can lead to an application crash, related to dav1d_decode_frame_exit.	CVE-2023-32570	Medium			debian:bookworm:libdav1d6	All Versions		0001-01-01T00:00:00Z	Not Covered
A Segmentation fault caused by a floating point exception exists in libheif 1.15.1 using crafted heif images via the heif::Fraction::round() function in box.cc, which causes a denial of service.	CVE-2023-29659	Medium			debian:bookworm:libheif1	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
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	Medium		sha256__adaa6238f46912e8d63b00b1f48b33d7a2a256ca20f094421876c2203e342b67.tar.gz/usr/bin/python3.11	python:python	<= 3.12.0a7		0001-01-01T00:00:00Z	Not Covered
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	Medium			debian:bookworm:python3.11	All Versions		0001-01-01T00:00:00Z	Not Covered
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	Medium			debian:bookworm:libpython3.11-minimal	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
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	Medium			debian:bookworm:libpython3.11-stdlib	All Versions		0001-01-01T00:00:00Z	Not Covered
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	Medium			debian:bookworm:python3.11-minimal	All Versions		0001-01-01T00:00:00Z	Not Covered
Multiple integer overflows in libgd in PHP before 5.2.4 allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a large (1) srcW or (2) srcH value to the (a) gdImageCopyResized function, or a large (3) sy (height) or (4) sx (width) value to the (b) gdImageCreate or the (c) gdImageCreateTrueColor function.	CVE-2007-3996	Medium			debian:bookworm:libwmflite-0.2-7	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The _gdGetColors function in gd_gd.c in PHP 5.2.11 and 5.3.x before 5.3.1, and the GD Graphics Library 2.x, does not properly verify a certain colorsTotal structure member, which might allow remote attackers to conduct buffer overflow or buffer over-read attacks via a crafted GD file, a different vulnerability than CVE-2009-3293. NOTE: some of these details are obtained from third party information.	CVE-2009-3546	Medium			debian:bookworm:libwmflite-0.2-7	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in ImageMagick. This security flaw cause a remote code execution vulnerability in OpenBlob with --enable-pipes configured.	CVE-2023-34152	Low	High		debian:bookworm:imagemagick-6-common	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in ImageMagick. This security flaw cause a remote code execution vulnerability in OpenBlob with --enable-pipes configured.	CVE-2023-34152	Low	High		debian:bookworm:libmagickcore-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in ImageMagick. This security flaw cause a remote code execution vulnerability in OpenBlob with --enable-pipes configured.	CVE-2023-34152	Low	High		debian:bookworm:libmagickwand-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in ImageMagick. This security flaw cause a remote code execution vulnerability in OpenBlob with --enable-pipes configured.	CVE-2023-34152	Low	High		debian:bookworm:libmagickcore-6.q16-6-extra	All Versions		0001-01-01T00:00:00Z	Not Covered
HTTP::Tiny before 0.083, a Perl core module since 5.13.9 and available standalone on CPAN, has an insecure default TLS configuration where users must opt in to verify certificates.	CVE-2023-31486	Low	High		debian:bookworm:perl	All Versions		0001-01-01T00:00:00Z	Not Covered
HTTP::Tiny before 0.083, a Perl core module since 5.13.9 and available standalone on CPAN, has an insecure default TLS configuration where users must opt in to verify certificates.	CVE-2023-31486	Low	High		debian:bookworm:libperl5.36	All Versions		0001-01-01T00:00:00Z	Not Covered
HTTP::Tiny before 0.083, a Perl core module since 5.13.9 and available standalone on CPAN, has an insecure default TLS configuration where users must opt in to verify certificates.	CVE-2023-31486	Low	High		debian:bookworm:perl-modules-5.36	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
HTTP::Tiny before 0.083, a Perl core module since 5.13.9 and available standalone on CPAN, has an insecure default TLS configuration where users must opt in to verify certificates.	CVE-2023-31486	Low	High		debian:bookworm:perl-base	All Versions		0001-01-01T00:00:00Z	Not Covered
It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the master keyring, leading to a potential man-in-the-middle attack.	CVE-2011-3374	Low	High		debian:bookworm:apt	All Versions		2023-01-08T19:25:00Z	Not Covered
It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the master keyring, leading to a potential man-in-the-middle attack.	CVE-2011-3374	Low	High		debian:bookworm:libapt-pkg6.0	All Versions		2023-01-08T19:25:00Z	Not Covered
In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\\1\\1|t1|\\\2537)+' in grep.	CVE-2018-20796	Low	Medium		debian:bookworm:libc6	All Versions		2023-01-08T19:31:00Z	Not Covered
In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\\1\\1|t1|\\\2537)+' in grep.	CVE-2018-20796	Low	Medium		debian:bookworm:libc-devtools	All Versions		2023-01-08T19:31:00Z	Not Covered
In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\\1\\1|t1|\\\2537)+' in grep.	CVE-2018-20796	Low	Medium		debian:bookworm:libc-dev-bin	All Versions		2023-01-08T19:31:00Z	Not Covered
In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\\1\\1|t1|\\\2537)+' in grep.	CVE-2018-20796	Low	Medium		debian:bookworm:libc-bin	All Versions		2023-01-08T19:31:00Z	Not Covered
In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\\1\\1)*' in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern	CVE-2019-9192	Low	Medium		debian:bookworm:libc-devtools	All Versions		2023-01-08T19:31:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\\1\\1)*' in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern	CVE-2019-9192	Low	Medium		debian:bookworm:libc-bin	All Versions		2023-01-08T19:31:00Z	Not Covered
In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\\1\\1)*' in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern	CVE-2019-9192	Low	Medium		debian:bookworm:libc6	All Versions		2023-01-08T19:31:00Z	Not Covered
In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\\1\\1)*' in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern	CVE-2019-9192	Low	Medium		debian:bookworm:libc-dev-bin	All Versions		2023-01-08T19:31:00Z	Not Covered
Parsing invalid messages can panic. Parsing a text-format message which contains a potential number consisting of a minus sign, one or more characters of whitespace, and no further input will cause a panic.	CVE-2023-24535	Low	Medium		debian:bookworm:libpython3.11-stdlib	All Versions		0001-01-01T00:00:00Z	Not Covered
Parsing invalid messages can panic. Parsing a text-format message which contains a potential number consisting of a minus sign, one or more characters of whitespace, and no further input will cause a panic.	CVE-2023-24535	Low	Medium		debian:bookworm:python3.11-minimal	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Parsing invalid messages can panic. Parsing a text-format message which contains a potential number consisting of a minus sign, one or more characters of whitespace, and no further input will cause a panic.	CVE-2023-24535	Low	Medium		debian:bookworm:libpython3.11-minimal	All Versions		0001-01-01T00:00:00Z	Not Covered
Parsing invalid messages can panic. Parsing a text-format message which contains a potential number consisting of a minus sign, one or more characters of whitespace, and no further input will cause a panic.	CVE-2023-24535	Low	Medium		debian:bookworm:python3.11	All Versions		0001-01-01T00:00:00Z	Not Covered
A heap-buffer-overflow vulnerability was found in LibTIFF, in extractImageSection() at tools/tiffcrop.c:7916 and tools/tiffcrop.c:7801. This flaw allows attackers to cause a denial of service via a crafted tiff file.	CVE-2023-3164	Low	Medium		debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.	CVE-2010-4756	Low	Medium		debian:bookworm:libc6	All Versions		2023-01-08T19:30:00Z	Not Covered
The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.	CVE-2010-4756	Low	Medium		debian:bookworm:libc-devtools	All Versions		2023-01-08T19:30:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.	CVE-2010-4756	Low	Medium		debian:bookworm:libc-dev-bin	All Versions		2023-01-08T19:30:00Z	Not Covered
The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.	CVE-2010-4756	Low	Medium		debian:bookworm:libc-bin	All Versions		2023-01-08T19:30:00Z	Not Covered
systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.	CVE-2013-4392	Low	Medium		debian:bookworm:systemd-sysv	All Versions		2023-01-08T19:25:00Z	Not Covered
systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.	CVE-2013-4392	Low	Medium		debian:bookworm:libsystemd-shared	All Versions		2023-01-08T19:25:00Z	Not Covered
systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.	CVE-2013-4392	Low	Medium		debian:bookworm:libudev1	All Versions		2023-01-08T19:25:00Z	Not Covered
systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.	CVE-2013-4392	Low	Medium		debian:bookworm:libnss-systemd	All Versions		2023-01-08T19:25:00Z	Not Covered
systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.	CVE-2013-4392	Low	Medium		debian:bookworm:libpam-systemd	All Versions		2023-01-08T19:25:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.	CVE-2013-4392	Low	Medium		debian:bookworm:udev	All Versions		2023-01-08T19:25:00Z	Not Covered
systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.	CVE-2013-4392	Low	Medium		debian:bookworm:systemd	All Versions		2023-01-08T19:25:00Z	Not Covered
systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.	CVE-2013-4392	Low	Medium		debian:bookworm:libsystemd0	All Versions		2023-01-08T19:25:00Z	Not Covered
systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.	CVE-2013-4392	Low	Medium		debian:bookworm:systemd-timesyncd	All Versions		2023-01-08T19:25:00Z	Not Covered
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-1010022	Low	Low		debian:bookworm:libc-devtools	All Versions		2023-01-08T19:25:00Z	Not Covered
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-1010022	Low	Low		debian:bookworm:libc-dev-bin	All Versions		2023-01-08T19:25:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-1010022	Low	Low		debian:bookworm:libc6	All Versions		2023-01-08T19:25:00Z	Not Covered
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-1010022	Low	Low		debian:bookworm:libc-bin	All Versions		2023-01-08T19:25:00Z	Not Covered
An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.	CVE-2018-5709	Low	Low		debian:bookworm:libkrb5-3	All Versions		2023-01-08T19:26:00Z	Not Covered
An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.	CVE-2018-5709	Low	Low		debian:bookworm:libk5crypto3	All Versions		2023-01-08T19:26:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.	CVE-2018-5709	Low	Low		debian:bookworm:krb5-locales	All Versions		2023-01-08T19:26:00Z	Not Covered
An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.	CVE-2018-5709	Low	Low		debian:bookworm:libgssapi-krb5-2	All Versions		2023-01-08T19:26:00Z	Not Covered
An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.	CVE-2018-5709	Low	Low		debian:bookworm:libkrb5support0	All Versions		2023-01-08T19:26:00Z	Not Covered
Tar 1.15.1 does not properly warn the user when extracting setuid or setgid files, which may allow local users or remote attackers to gain privileges.	CVE-2005-2541	Low	Low		debian:bookworm:tar	All Versions		2023-01-08T19:25:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bookworm:bsdutils	All Versions		2023-01-08T19:26:00Z	Not Covered
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bookworm:util-linux-extra	All Versions		2023-01-08T19:26:00Z	Not Covered
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bookworm:libuuid1	All Versions		2023-01-08T19:26:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bookworm:bsdextrautils	All Versions		2023-01-08T19:26:00Z	Not Covered
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bookworm:libmount1	All Versions		2023-01-08T19:26:00Z	Not Covered
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bookworm:libfdisk1	All Versions		2023-01-08T19:26:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bookworm:libblkid1	All Versions		2023-01-08T19:26:00Z	Not Covered
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bookworm:mount	All Versions		2023-01-08T19:26:00Z	Not Covered
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bookworm:fdisk	All Versions		2023-01-08T19:26:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bookworm:eject	All Versions		2023-01-08T19:26:00Z	Not Covered
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bookworm:util-linux	All Versions		2023-01-08T19:26:00Z	Not Covered
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bookworm:libsmartcols1	All Versions		2023-01-08T19:26:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
shadow 4.8, in certain circumstances affecting at least Gentoo, Arch Linux, and Void Linux, allows local users to obtain root access because setuid programs are misconfigured. Specifically, this affects shadow 4.8 when compiled using --with-libpam but without explicitly passing --disable-account-tools-setuid, and without a PAM configuration suitable for use with setuid account management tools. This combination leads to account management tools (groupadd, groupdel, groupmod, useradd, userdel, usermod) that can easily be used by unprivileged local users to escalate privileges to root in multiple ways. This issue became much more relevant in approximately December 2019 when an unrelated bug was fixed (i.e., the chmod calls to suidusbins were fixed in the upstream Makefile which is now included in the release version 4.8).	CVE-2019-19882	Low			debian:bookworm:passwd	All Versions		0001-01-01T00:00:00Z	Not Covered
shadow 4.8, in certain circumstances affecting at least Gentoo, Arch Linux, and Void Linux, allows local users to obtain root access because setuid programs are misconfigured. Specifically, this affects shadow 4.8 when compiled using --with-libpam but without explicitly passing --disable-account-tools-setuid, and without a PAM configuration suitable for use with setuid account management tools. This combination leads to account management tools (groupadd, groupdel, groupmod, useradd, userdel, usermod) that can easily be used by unprivileged local users to escalate privileges to root in multiple ways. This issue became much more relevant in approximately December 2019 when an unrelated bug was fixed (i.e., the chmod calls to suidusbins were fixed in the upstream Makefile which is now included in the release version 4.8).	CVE-2019-19882	Low			debian:bookworm:login	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc. NOTE: the vendor's position is "ASLR bypass itself is not a vulnerability.	CVE-2019-10 10025	Low			debian:bookworm:libc-bin	All Versions		0001-01-01T00: 00:00Z	Not Covered
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc. NOTE: the vendor's position is "ASLR bypass itself is not a vulnerability.	CVE-2019-10 10025	Low			debian:bookworm:libc6	All Versions		0001-01-01T00: 00:00Z	Not Covered
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc. NOTE: the vendor's position is "ASLR bypass itself is not a vulnerability.	CVE-2019-10 10025	Low			debian:bookworm:libc-devtools	All Versions		0001-01-01T00: 00:00Z	Not Covered
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc. NOTE: the vendor's position is "ASLR bypass itself is not a vulnerability.	CVE-2019-10 10025	Low			debian:bookworm:libc-dev-bin	All Versions		0001-01-01T00: 00:00Z	Not Covered
GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-10 10023	Low			debian:bookworm:libc-bin	All Versions		0001-01-01T00: 00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-10 10023	Low			debian:bookworm:libc6	All Versions		0001-01-01T00: 00:00Z	Not Covered
GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-10 10023	Low			debian:bookworm:libc-devtools	All Versions		0001-01-01T00: 00:00Z	Not Covered
GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-10 10023	Low			debian:bookworm:libc-dev-bin	All Versions		0001-01-01T00: 00:00Z	Not Covered
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-10 10024	Low			debian:bookworm:libc-devtools	All Versions		0001-01-01T00: 00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-1010024	Low			debian:bookworm:libc-bin	All Versions		0001-01-01T00:00:00Z	Not Covered
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-1010024	Low			debian:bookworm:libc-dev-bin	All Versions		0001-01-01T00:00:00Z	Not Covered
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-1010024	Low			debian:bookworm:libc6	All Versions		0001-01-01T00:00:00Z	Not Covered
Out-of-bounds accesses in the functions pi_next_lrcp, pi_next_rlcp, pi_next_rpcl, pi_next_pcrl, pi_next_rpcl, and pi_next_cprl in openmj2/pi.c in OpenJPEG through 2.3.0 allow remote attackers to cause a denial of service (application crash).	CVE-2018-20846	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered
In all versions of AppArmor mount rules are accidentally widened when compiled.	CVE-2016-1585	Low			debian:bookworm:libapparmor1	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in OpenJPEG 2.3.0. It allows remote attackers to cause a denial of service (attempted excessive memory allocation) in opj_calloc in openjp2/opj_malloc.c, when called from opj_tcd_init_tile in openjp2/tcd.c, as demonstrated by the 64-bit opj_decompress.	CVE-2019-6988	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31.1. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by c++filt.	CVE-2018-20712	Low			debian:bookworm:libbinutils	All Versions		0001-01-01T00:00:00Z	Not Covered
A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31.1. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by c++filt.	CVE-2018-20712	Low			debian:bookworm:libctf0	All Versions		0001-01-01T00:00:00Z	Not Covered
A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31.1. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by c++filt.	CVE-2018-20712	Low			debian:bookworm:binutils-x86-64-linux-gnu	All Versions		0001-01-01T00:00:00Z	Not Covered
A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31.1. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by c++filt.	CVE-2018-20712	Low			debian:bookworm:libgprofng0	All Versions		0001-01-01T00:00:00Z	Not Covered
A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31.1. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by c++filt.	CVE-2018-20712	Low			debian:bookworm:libctf-nobfd0	All Versions		0001-01-01T00:00:00Z	Not Covered
A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31.1. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by c++filt.	CVE-2018-20712	Low			debian:bookworm:binutils-common	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31.1. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by c++filt.	CVE-2018-20712	Low			debian:bookworm:binutils	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in cairo 1.16.0. There is an assertion problem in the function _cairo_arc_in_direction in the file cairo-arc.c.	CVE-2019-6461	Low			debian:bookworm:libcairo-gobject2	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in cairo 1.16.0. There is an assertion problem in the function _cairo_arc_in_direction in the file cairo-arc.c.	CVE-2019-6461	Low			debian:bookworm:libcairo2	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in cairo 1.16.0. There is an infinite loop in the function _arc_error_normalized in the file cairo-arc.c, related to _arc_max_angle_for_tolerance_normalized.	CVE-2019-6462	Low			debian:bookworm:libcairo-gobject2	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in cairo 1.16.0. There is an infinite loop in the function _arc_error_normalized in the file cairo-arc.c, related to _arc_max_angle_for_tolerance_normalized.	CVE-2019-6462	Low			debian:bookworm:libcairo2	All Versions		0001-01-01T00:00:00Z	Not Covered
The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.	CVE-2018-20673	Low			debian:bookworm:binutils-x86-64-linux-gnu	All Versions		0001-01-01T00:00:00Z	Not Covered
The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.	CVE-2018-20673	Low			debian:bookworm:binutils-common	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.	CVE-2018-20673	Low			debian:bookworm:libbinutils	All Versions		0001-01-01T00:00:00Z	Not Covered
The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.	CVE-2018-20673	Low			debian:bookworm:libgprofng0	All Versions		0001-01-01T00:00:00Z	Not Covered
The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.	CVE-2018-20673	Low			debian:bookworm:binutils	All Versions		0001-01-01T00:00:00Z	Not Covered
The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.	CVE-2018-20673	Low			debian:bookworm:libctf-nobfd0	All Versions		0001-01-01T00:00:00Z	Not Covered
The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.	CVE-2018-20673	Low			debian:bookworm:libctf0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The get_count function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31, allows remote attackers to cause a denial of service (malloc called with the result of an integer-overflowing calculation) or possibly have unspecified other impact via a crafted string, as demonstrated by c++filt.	CVE-2018-18483	Low			debian:bookworm:binutils-x86-64-linux-gnu	All Versions		0001-01-01T00:00:00Z	Not Covered
The get_count function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31, allows remote attackers to cause a denial of service (malloc called with the result of an integer-overflowing calculation) or possibly have unspecified other impact via a crafted string, as demonstrated by c++filt.	CVE-2018-18483	Low			debian:bookworm:binutils-common	All Versions		0001-01-01T00:00:00Z	Not Covered
The get_count function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31, allows remote attackers to cause a denial of service (malloc called with the result of an integer-overflowing calculation) or possibly have unspecified other impact via a crafted string, as demonstrated by c++filt.	CVE-2018-18483	Low			debian:bookworm:libbinutils	All Versions		0001-01-01T00:00:00Z	Not Covered
The get_count function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31, allows remote attackers to cause a denial of service (malloc called with the result of an integer-overflowing calculation) or possibly have unspecified other impact via a crafted string, as demonstrated by c++filt.	CVE-2018-18483	Low			debian:bookworm:binutils	All Versions		0001-01-01T00:00:00Z	Not Covered
The get_count function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31, allows remote attackers to cause a denial of service (malloc called with the result of an integer-overflowing calculation) or possibly have unspecified other impact via a crafted string, as demonstrated by c++filt.	CVE-2018-18483	Low			debian:bookworm:libctf-nobfd0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The get_count function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31, allows remote attackers to cause a denial of service (malloc called with the result of an integer-overflowing calculation) or possibly have unspecified other impact via a crafted string, as demonstrated by c++filt.	CVE-2018-18483	Low			debian:bookworm:libctf0	All Versions		0001-01-01T00:00:00Z	Not Covered
The get_count function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31, allows remote attackers to cause a denial of service (malloc called with the result of an integer-overflowing calculation) or possibly have unspecified other impact via a crafted string, as demonstrated by c++filt.	CVE-2018-18483	Low			debian:bookworm:libgprofng0	All Versions		0001-01-01T00:00:00Z	Not Covered
cairo through 1.15.14 has an out-of-bounds stack-memory write during processing of a crafted document by WebKitGTK+ because of the interaction between cairo-rectangular-scan-converter.c (the generate and render_rows functions) and cairo-image-compositor.c (the _cairo_image_spans_and_zero function).	CVE-2018-18064	Low			debian:bookworm:libcairo2	All Versions		0001-01-01T00:00:00Z	Not Covered
cairo through 1.15.14 has an out-of-bounds stack-memory write during processing of a crafted document by WebKitGTK+ because of the interaction between cairo-rectangular-scan-converter.c (the generate and render_rows functions) and cairo-image-compositor.c (the _cairo_image_spans_and_zero function).	CVE-2018-18064	Low			debian:bookworm:libcairo-gobject2	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in OpenJPEG 2.3.0. A heap-based buffer overflow was discovered in the function t2_encode_packet in lib/openmj2/t2.c. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service or possibly unspecified other impact.	CVE-2018-16376	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in OpenJPEG 2.3.0. Missing checks for header_info.height and header_info.width in the function pnmtoimage in bin/jpwl/convert.c can lead to a heap-based buffer overflow.	CVE-2018-16375	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered
In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x36 0x36 0x36 0x36 0x36 0x36 0x1f 0x35 0x50 0x00 can result in a hang of several minutes during which CPU and memory resources are consumed until ultimately an attempted large memory allocation fails. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted file.	CVE-2018-15607	Low			debian:bookworm:libmagickcore-6.q16-6-extra	All Versions		0001-01-01T00:00:00Z	Not Covered
In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x36 0x36 0x36 0x36 0x36 0x36 0x1f 0x35 0x50 0x00 can result in a hang of several minutes during which CPU and memory resources are consumed until ultimately an attempted large memory allocation fails. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted file.	CVE-2018-15607	Low			debian:bookworm:libmagickwand-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x36 0x36 0x36 0x36 0x36 0x36 0x1f 0x35 0x50 0x00 can result in a hang of several minutes during which CPU and memory resources are consumed until ultimately an attempted large memory allocation fails. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted file.	CVE-2018-15607	Low			debian:bookworm:imagemagick-6-common	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x36 0x36 0x36 0x36 0x36 0x36 0x1f 0x35 0x50 0x00 can result in a hang of several minutes during which CPU and memory resources are consumed until ultimately an attempted large memory allocation fails. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted file.	CVE-2018-15607	Low			debian:bookworm:libmagickcore-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
ARM mbedTLS version 2.7.0 and earlier contains a Ciphersuite Allows Incorrectly Signed Certificates vulnerability in mbedtls_ssl_get_verify_result() that can result in ECDSA-signed certificates are accepted, when only RSA-signed ones should be.. This attack appear to be exploitable via Peers negotiate a TLS-ECDH-RSA-* ciphersuite. Any of the peers can then provide an ECDSA-signed certificate, when only an RSA-signed one should be accepted..	CVE-2018-1000520	Low			debian:bookworm:libmbedcrypto7	All Versions		0001-01-01T00:00:00Z	Not Covered
LibTIFF 4.0.9 has a NULL pointer dereference in the jpeg_fdct_16x16 function in jfdctint.c.	CVE-2018-10126	Low			debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_template_value_parm, demangle_integral_value, and demangle_expression.	CVE-2018-9996	Low			debian:bookworm:libbinutils	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_template_value_parm, demangle_integral_value, and demangle_expression.	CVE-2018-9996	Low			debian:bookworm:binutils	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_template_value_parm, demangle_integral_value, and demangle_expression.	CVE-2018-9996	Low			debian:bookworm:libctf0	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_template_value_parm, demangle_integral_value, and demangle_expression.	CVE-2018-9996	Low			debian:bookworm:libgprofng0	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_template_value_parm, demangle_integral_value, and demangle_expression.	CVE-2018-9996	Low			debian:bookworm:binutils-x86-64-linux-gnu	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_template_value_parm, demangle_integral_value, and demangle_expression.	CVE-2018-9996	Low			debian:bookworm:binutils-common	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_template_value_parm, demangle_integral_value, and demangle_expression.	CVE-2018-9996	Low			debian:bookworm:libctf-nobfd0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
cipher/elgamal.c in Libgcrypt through 1.8.2, when used to encrypt messages directly, improperly encodes plaintexts, which allows attackers to obtain sensitive information by reading ciphertext data (i.e., it does not have semantic security in face of a ciphertext-only attack). The Decisional Diffie-Hellman (DDH) assumption does not hold for Libgcrypt's ElGamal implementation.	CVE-2018-6829	Low			debian:bookworm:libgcrypt20	All Versions		0001-01-01T00:00:00Z	Not Covered
It was found that system umask policy is not being honored when creating XDG user directories, since Xsession sources xdg-user-dirs.sh before setting umask policy. This only affects xdg-user-dirs before 0.15.5 as shipped with Red Hat Enterprise Linux.	CVE-2017-15131	Low			debian:bookworm:xdg-user-dirs	All Versions		0001-01-01T00:00:00Z	Not Covered
In LibTIFF 4.0.8, there is a heap-based use-after-free in the t2p_writeproc function in tiff2pdf.c. NOTE: there is a third-party report of inability to reproduce this issue	CVE-2017-17973	Low			debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
contrib/slapd-modules/nops/nops.c in OpenLDAP through 2.4.45, when both the nops module and the memberof overlay are enabled, attempts to free a buffer that was allocated on the stack, which allows remote attackers to cause a denial of service (slapd crash) via a member MODDN operation.	CVE-2017-17740	Low			debian:bookworm:libldap-common	All Versions		0001-01-01T00:00:00Z	Not Covered
contrib/slapd-modules/nops/nops.c in OpenLDAP through 2.4.45, when both the nops module and the memberof overlay are enabled, attempts to free a buffer that was allocated on the stack, which allows remote attackers to cause a denial of service (slapd crash) via a member MODDN operation.	CVE-2017-17740	Low			debian:bookworm:libldap-2.5-0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
In GNU Coreutils through 8.29, chown-core.c in chown and chgrp does not prevent replacement of a plain file with a symlink during use of the POSIX "-R -L" options, which allows local users to modify the ownership of arbitrary files by leveraging a race condition.	CVE-2017-18018	Low			debian:bookworm:coreutils	All Versions		0001-01-01T00:00:00Z	Not Covered
In OpenJPEG 2.3.0, a stack-based buffer overflow was discovered in the pgxtoimage function in jpwl/convert.c. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service or possibly remote code execution.	CVE-2017-17479	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in xmllint (from libxml2) before 2.11.8 and 2.12.x before 2.12.7. Formatting error messages with xmllint --htmlout can result in a buffer over-read in xmlHTMLPrintFileContext in xmllint.c.	CVE-2024-34459	Low			debian:bookworm:libxml2	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa 23.0.4 was discovered to contain a buffer over-read in glXQueryServerString(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45919	Low			debian:bookworm:mesa-vdpau-drivers	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa 23.0.4 was discovered to contain a buffer over-read in glXQueryServerString(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45919	Low			debian:bookworm:mesa-va-drivers	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa 23.0.4 was discovered to contain a buffer over-read in glXQueryServerString(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45919	Low			debian:bookworm:mesa-vulkan-drivers	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Mesa 23.0.4 was discovered to contain a buffer over-read in glXQueryServerString(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45919	Low			debian:bookworm:libgl1-mesa-dri	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa 23.0.4 was discovered to contain a buffer over-read in glXQueryServerString(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45919	Low			debian:bookworm:libegl-mesa0	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa 23.0.4 was discovered to contain a buffer over-read in glXQueryServerString(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45919	Low			debian:bookworm:libglapi-mesa	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa 23.0.4 was discovered to contain a buffer over-read in glXQueryServerString(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45919	Low			debian:bookworm:libglx-mesa0	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa 23.0.4 was discovered to contain a buffer over-read in glXQueryServerString(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45919	Low			debian:bookworm:libgbm1	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Mesa v23.0.4 was discovered to contain a NULL pointer dereference via the function dri2GetGlxDrawableFromXDrawableId(). This vulnerability is triggered when the X11 server sends an DRI2_BufferSwapComplete event unexpectedly when the application is using DRI3. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45913	Low			debian:bookworm:libglapi-mesa	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa v23.0.4 was discovered to contain a NULL pointer dereference via the function dri2GetGlxDrawableFromXDrawableId(). This vulnerability is triggered when the X11 server sends an DRI2_BufferSwapComplete event unexpectedly when the application is using DRI3. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45913	Low			debian:bookworm:libglx-mesa0	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa v23.0.4 was discovered to contain a NULL pointer dereference via the function dri2GetGlxDrawableFromXDrawableId(). This vulnerability is triggered when the X11 server sends an DRI2_BufferSwapComplete event unexpectedly when the application is using DRI3. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45913	Low			debian:bookworm:mesa-va-drivers	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa v23.0.4 was discovered to contain a NULL pointer dereference via the function dri2GetGlxDrawableFromXDrawableId(). This vulnerability is triggered when the X11 server sends an DRI2_BufferSwapComplete event unexpectedly when the application is using DRI3. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45913	Low			debian:bookworm:libgbm1	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Mesa v23.0.4 was discovered to contain a NULL pointer dereference via the function dri2GetGlxDrawableFromXDrawableId(). This vulnerability is triggered when the X11 server sends an DRI2_BufferSwapComplete event unexpectedly when the application is using DRI3. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45913	Low			debian:bookworm:libegl-mesa0	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa v23.0.4 was discovered to contain a NULL pointer dereference via the function dri2GetGlxDrawableFromXDrawableId(). This vulnerability is triggered when the X11 server sends an DRI2_BufferSwapComplete event unexpectedly when the application is using DRI3. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45913	Low			debian:bookworm:libgl1-mesa-dri	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa v23.0.4 was discovered to contain a NULL pointer dereference via the function dri2GetGlxDrawableFromXDrawableId(). This vulnerability is triggered when the X11 server sends an DRI2_BufferSwapComplete event unexpectedly when the application is using DRI3. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45913	Low			debian:bookworm:mesa-vdpau-drivers	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa v23.0.4 was discovered to contain a NULL pointer dereference via the function dri2GetGlxDrawableFromXDrawableId(). This vulnerability is triggered when the X11 server sends an DRI2_BufferSwapComplete event unexpectedly when the application is using DRI3. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45913	Low			debian:bookworm:mesa-vulkan-drivers	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Mesa 23.0.4 was discovered to contain a NULL pointer dereference in check_xshm() for the has_error state. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45931	Low			debian:bookworm:mesa-vulkan-drivers	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa 23.0.4 was discovered to contain a NULL pointer dereference in check_xshm() for the has_error state. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45931	Low			debian:bookworm:mesa-vdpau-drivers	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa 23.0.4 was discovered to contain a NULL pointer dereference in check_xshm() for the has_error state. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45931	Low			debian:bookworm:libglx-mesa0	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa 23.0.4 was discovered to contain a NULL pointer dereference in check_xshm() for the has_error state. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45931	Low			debian:bookworm:libgbm1	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa 23.0.4 was discovered to contain a NULL pointer dereference in check_xshm() for the has_error state. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45931	Low			debian:bookworm:libglapi-mesa	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa 23.0.4 was discovered to contain a NULL pointer dereference in check_xshm() for the has_error state. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45931	Low			debian:bookworm:libegl-mesa0	All Versions		0001-01-01T00:00:00Z	Not Covered
Mesa 23.0.4 was discovered to contain a NULL pointer dereference in check_xshm() for the has_error state. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45931	Low			debian:bookworm:mesa-va-drivers	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Mesa 23.0.4 was discovered to contain a NULL pointer dereference in check_xshm() for the has_error state. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.	CVE-2023-45931	Low			debian:bookworm:libgl1-mesa-dri	All Versions		0001-01-01T00:00:00Z	Not Covered
S-Lang 2.3.2 was discovered to contain a segmentation fault via the function fixup_tgetstr().	CVE-2023-45929	Low			debian:bookworm:libslang2	All Versions		0001-01-01T00:00:00Z	Not Covered
S-Lang 2.3.2 was discovered to contain an arithmetic exception via the function tt_sprintf().	CVE-2023-45927	Low			debian:bookworm:libslang2	All Versions		0001-01-01T00:00:00Z	Not Covered
libglxproto.c in OpenGL libglvnd bb06db5a was discovered to contain a segmentation violation via the function glXGetDrawableScreen(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45924	Low			debian:bookworm:libglvnd0	All Versions		0001-01-01T00:00:00Z	Not Covered
libglxproto.c in OpenGL libglvnd bb06db5a was discovered to contain a segmentation violation via the function glXGetDrawableScreen(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45924	Low			debian:bookworm:libglx0	All Versions		0001-01-01T00:00:00Z	Not Covered
libglxproto.c in OpenGL libglvnd bb06db5a was discovered to contain a segmentation violation via the function glXGetDrawableScreen(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45924	Low			debian:bookworm:libgles2	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
libglxproto.c in OpenGL libglvnd bb06db5a was discovered to contain a segmentation violation via the function glXGetDrawableScreen(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45924	Low			debian:bookworm:libegl1	All Versions		0001-01-01T00:00:00Z	Not Covered
libglxproto.c in OpenGL libglvnd bb06db5a was discovered to contain a segmentation violation via the function glXGetDrawableScreen(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45924	Low			debian:bookworm:libgl1	All Versions		0001-01-01T00:00:00Z	Not Covered
glx_pbuffer.c in Mesa 23.0.4 was discovered to contain a segmentation violation when calling __glXGetDrawableAttribute(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45922	Low			debian:bookworm:libgbm1	All Versions		0001-01-01T00:00:00Z	Not Covered
glx_pbuffer.c in Mesa 23.0.4 was discovered to contain a segmentation violation when calling __glXGetDrawableAttribute(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45922	Low			debian:bookworm:libgl1-mesa-dri	All Versions		0001-01-01T00:00:00Z	Not Covered
glx_pbuffer.c in Mesa 23.0.4 was discovered to contain a segmentation violation when calling __glXGetDrawableAttribute(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45922	Low			debian:bookworm:mesa-va-drivers	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
glx_pbuffer.c in Mesa 23.0.4 was discovered to contain a segmentation violation when calling __glXGetDrawableAttribute(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45922	Low			debian:bookworm:mesa-vdpau-drivers	All Versions		0001-01-01T00:00:00Z	Not Covered
glx_pbuffer.c in Mesa 23.0.4 was discovered to contain a segmentation violation when calling __glXGetDrawableAttribute(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45922	Low			debian:bookworm:libglapi-mesa	All Versions		0001-01-01T00:00:00Z	Not Covered
glx_pbuffer.c in Mesa 23.0.4 was discovered to contain a segmentation violation when calling __glXGetDrawableAttribute(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45922	Low			debian:bookworm:mesa-vulkan-drivers	All Versions		0001-01-01T00:00:00Z	Not Covered
glx_pbuffer.c in Mesa 23.0.4 was discovered to contain a segmentation violation when calling __glXGetDrawableAttribute(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45922	Low			debian:bookworm:libegl-mesa0	All Versions		0001-01-01T00:00:00Z	Not Covered
glx_pbuffer.c in Mesa 23.0.4 was discovered to contain a segmentation violation when calling __glXGetDrawableAttribute(). NOTE: this is disputed because there are no common situations in which users require uninterrupted operation with an attacker-controller server.	CVE-2023-45922	Low			debian:bookworm:libglx-mesa0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
libcurl skips the certificate verification for a QUIC connection under certain conditions, when built to use wolfSSL. If told to use an unknown/bad cipher or curve, the error path accidentally skips the verification and returns OK, thus ignoring any certificate problems.	CVE-2024-2379	Low			debian:bookworm:libcurl3-gnutls	All Versions		0001-01-01T00:00:00Z	Not Covered
LibTIFF 4.0.8 has multiple memory leak vulnerabilities, which allow attackers to cause a denial of service (memory consumption), as demonstrated by tif_open.c, tif_lzw.c, and tif_aux.c. NOTE: Third parties were unable to reproduce the issue	CVE-2017-16232	Low			debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
libexpat through 2.6.1 allows an XML Entity Expansion attack when there is isolated use of external parsers (created via XML_ExternalEntityParserCreate).	CVE-2024-28757	Low			debian:bookworm:libexpat1	All Versions		0001-01-01T00:00:00Z	Not Covered
libheif <= 1.17.6 contains a memory leak in the function JpegEncoder::Encode. This flaw allows an attacker to cause a denial of service attack.	CVE-2024-25269	Low			debian:bookworm:libheif1	All Versions		0001-01-01T00:00:00Z	Not Covered
elfutils v0.189 was discovered to contain a NULL pointer dereference via the handle_verdef() function at readelf.c.	CVE-2024-25260	Low			debian:bookworm:libdw1	All Versions		0001-01-01T00:00:00Z	Not Covered
elfutils v0.189 was discovered to contain a NULL pointer dereference via the handle_verdef() function at readelf.c.	CVE-2024-25260	Low			debian:bookworm:libelf1	All Versions		0001-01-01T00:00:00Z	Not Covered
libexpat through 2.5.0 allows recursive XML Entity Expansion if XML_DTD is undefined at compile time.	CVE-2023-52426	Low			debian:bookworm:libexpat1	All Versions		0001-01-01T00:00:00Z	Not Covered
Ubuntu's pipewire-pulse in snap grants microphone access even when the snap interface for audio-record is not set.	CVE-2022-4964	Low			debian:bookworm:libpipewire-0.3-0	All Versions		0001-01-01T00:00:00Z	Not Covered
Ubuntu's pipewire-pulse in snap grants microphone access even when the snap interface for audio-record is not set.	CVE-2022-4964	Low			debian:bookworm:libspa-0.2-modules	All Versions		0001-01-01T00:00:00Z	Not Covered
Ubuntu's pipewire-pulse in snap grants microphone access even when the snap interface for audio-record is not set.	CVE-2022-4964	Low			debian:bookworm:libpipewire-0.3-common	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Header::readfrom in IlmImf/ImfHeader.cpp in OpenEXR 2.2.0 allows remote attackers to cause a denial of service (excessive memory allocation) via a crafted file that is accessed with the ImfOpenInputFile function in IlmImf/ImfCRgbaFile.cpp. NOTE: The maintainer and multiple third parties believe that this vulnerability isn't valid	CVE-2017-14988	Low			debian:bookworm:libopenexr-3-1-30	All Versions		0001-01-01T00:00:00Z	Not Covered
slapd in OpenLDAP 2.4.45 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill `cat /pathname`" command, as demonstrated by openldap-initscript.	CVE-2017-14159	Low			debian:bookworm:libldap-common	All Versions		0001-01-01T00:00:00Z	Not Covered
slapd in OpenLDAP 2.4.45 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill `cat /pathname`" command, as demonstrated by openldap-initscript.	CVE-2017-14159	Low			debian:bookworm:libldap-2.5-0	All Versions		0001-01-01T00:00:00Z	Not Covered
Heap-based buffer overflow in the alloc_segs function in lib/dbm/src/hash.c in Mozilla Network Security Services (NSS) allows context-dependent attackers to have unspecified impact using a crafted cert8.db file.	CVE-2017-11695	Low			debian:bookworm:libnss3	All Versions		0001-01-01T00:00:00Z	Not Covered
Heap-based buffer overflow in the __get_page function in lib/dbm/src/h_page.c in Mozilla Network Security Services (NSS) allows context-dependent attackers to have unspecified impact using a crafted cert8.db file.	CVE-2017-11698	Low			debian:bookworm:libnss3	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted file, as demonstrated by a call from the Binary File Descriptor (BFD) library (aka libbfd).	CVE-2017-13716	Low			debian:bookworm:libctf0	All Versions		0001-01-01T00:00:00Z	Not Covered
The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted file, as demonstrated by a call from the Binary File Descriptor (BFD) library (aka libbfd).	CVE-2017-13716	Low			debian:bookworm:libctf-nobfd0	All Versions		0001-01-01T00:00:00Z	Not Covered
The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted file, as demonstrated by a call from the Binary File Descriptor (BFD) library (aka libbfd).	CVE-2017-13716	Low			debian:bookworm:libbinutils	All Versions		0001-01-01T00:00:00Z	Not Covered
The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted file, as demonstrated by a call from the Binary File Descriptor (BFD) library (aka libbfd).	CVE-2017-13716	Low			debian:bookworm:binutils-common	All Versions		0001-01-01T00:00:00Z	Not Covered
The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted file, as demonstrated by a call from the Binary File Descriptor (BFD) library (aka libbfd).	CVE-2017-13716	Low			debian:bookworm:binutils	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted file, as demonstrated by a call from the Binary File Descriptor (BFD) library (aka libbfd).	CVE-2017-13716	Low			debian:bookworm:libgprofng0	All Versions		0001-01-01T00:00:00Z	Not Covered
The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted file, as demonstrated by a call from the Binary File Descriptor (BFD) library (aka libbfd).	CVE-2017-13716	Low			debian:bookworm:binutils-x86-64-linux-gnu	All Versions		0001-01-01T00:00:00Z	Not Covered
Heap-based buffer overflow in the __hash_open function in lib/dbm/src/hash.c in Mozilla Network Security Services (NSS) allows context-dependent attackers to have unspecified impact using a crafted cert8.db file.	CVE-2017-11696	Low			debian:bookworm:libnss3	All Versions		0001-01-01T00:00:00Z	Not Covered
Division-by-zero vulnerabilities in the functions opj_pi_next_cprl, opj_pi_next_pcrl, and opj_pi_next_rpcl in pi.c in OpenJPEG before 2.2.0 allow remote attackers to cause a denial of service (application crash) via crafted j2k files.	CVE-2016-10506	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered
The __hash_open function in hash.c:229 in Mozilla Network Security Services (NSS) allows context-dependent attackers to cause a denial of service (floating point exception and crash) via a crafted cert8.db file.	CVE-2017-11697	Low			debian:bookworm:libnss3	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
NULL pointer dereference vulnerabilities in the imagetopnm function in convert.c, sycc444_to_rgb function in color.c, color_esycc_to_rgb function in color.c, and sycc422_to_rgb function in color.c in OpenJPEG before 2.2.0 allow remote attackers to cause a denial of service (application crash) via crafted j2k files.	CVE-2016-10505	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered
A remote denial of service vulnerability in libvpx in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-34360591.	CVE-2017-0641	Low			debian:bookworm:libvpx7	All Versions		0001-01-01T00:00:00Z	Not Covered
The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file that is mishandled in an AcquireSemaphoreInfo call.	CVE-2017-11755	Low			debian:bookworm:imagemagick-6-common	All Versions		0001-01-01T00:00:00Z	Not Covered
The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file that is mishandled in an AcquireSemaphoreInfo call.	CVE-2017-11755	Low			debian:bookworm:libmagickcore-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file that is mishandled in an AcquireSemaphoreInfo call.	CVE-2017-11755	Low			debian:bookworm:libmagickwand-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file that is mishandled in an AcquireSemaphoreInfo call.	CVE-2017-11755	Low			debian:bookworm:libmagickcore-6.q16-6-extra	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file that is mishandled in an OpenPixelCache call.	CVE-2017-11754	Low			debian:bookworm:libmagickcore-6.q16-6-extra	All Versions		0001-01-01T00:00:00Z	Not Covered
The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file that is mishandled in an OpenPixelCache call.	CVE-2017-11754	Low			debian:bookworm:imagemagick-6-common	All Versions		0001-01-01T00:00:00Z	Not Covered
The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file that is mishandled in an OpenPixelCache call.	CVE-2017-11754	Low			debian:bookworm:libmagickwand-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file that is mishandled in an OpenPixelCache call.	CVE-2017-11754	Low			debian:bookworm:libmagickcore-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
In LibTIFF 4.0.8, there is a memory malloc failure in tif_jbig.c. A crafted TIFF document can lead to an abort resulting in a remote denial of service attack.	CVE-2017-9937	Low			debian:bookworm:libjbig0	All Versions		0001-01-01T00:00:00Z	Not Covered
Cairo version 1.15.4 is vulnerable to a NULL pointer dereference related to the FT_Load_Glyph and FT_Render_Glyph resulting in an application crash.	CVE-2017-7475	Low			debian:bookworm:libcairo2	All Versions		0001-01-01T00:00:00Z	Not Covered
Cairo version 1.15.4 is vulnerable to a NULL pointer dereference related to the FT_Load_Glyph and FT_Render_Glyph resulting in an application crash.	CVE-2017-7475	Low			debian:bookworm:libcairo-gobject2	All Versions		0001-01-01T00:00:00Z	Not Covered
In LibTIFF 4.0.7, the program processes BMP images without verifying that biWidth and biHeight in the bitmap-information header match the actual input, leading to a heap-based buffer over-read in bmp2tiff.	CVE-2017-9117	Low			debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
cJSON v1.7.16 was discovered to contain a segmentation violation via the function cJSON_SetValuestring at cJSON.c.	CVE-2023-50472	Low			debian:bookworm:libcjson1	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was found in the tiffcp utility distributed by the libtiff package where a crafted TIFF file on processing may cause a heap-based buffer overflow leads to an application crash.	CVE-2023-6228	Low			debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
Mbed TLS 2.x before 2.28.5 and 3.x before 3.5.0 has a Buffer Overflow.	CVE-2023-43615	Low			debian:bookworm:libmbedcrypto7	All Versions		0001-01-01T00:00:00Z	Not Covered
In libxslt 1.1.29 and earlier, the EXSLT math.random function was not initialized with a random seed during startup, which could cause usage of this function to produce predictable outputs.	CVE-2015-9019	Low			debian:bookworm:libxslt1.1	All Versions		0001-01-01T00:00:00Z	Not Covered
The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers to cause a denial of service (attempted large memory allocation and application crash) via a crafted file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8862 and CVE-2016-8866.	CVE-2017-7275	Low			debian:bookworm:libmagickcore-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers to cause a denial of service (attempted large memory allocation and application crash) via a crafted file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8862 and CVE-2016-8866.	CVE-2017-7275	Low			debian:bookworm:imagemagick-6-common	All Versions		0001-01-01T00:00:00Z	Not Covered
The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers to cause a denial of service (attempted large memory allocation and application crash) via a crafted file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8862 and CVE-2016-8866.	CVE-2017-7275	Low			debian:bookworm:libmagickwand-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers to cause a denial of service (attempted large memory allocation and application crash) via a crafted file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8862 and CVE-2016-8866.	CVE-2017-7275	Low			debian:bookworm:libmagickcore-6.q16-6-extra	All Versions		0001-01-01T00:00:00Z	Not Covered
Under some circumstances, this weakness allows a user who has access to run the â€œpsâ€• utility on a machine, the ability to write almost unlimited amounts of unfiltered data into the process heap.	CVE-2023-4016	Low			debian:bookworm:libproc2-0	All Versions		0001-01-01T00:00:00Z	Not Covered
Under some circumstances, this weakness allows a user who has access to run the â€œpsâ€• utility on a machine, the ability to write almost unlimited amounts of unfiltered data into the process heap.	CVE-2023-4016	Low			debian:bookworm:procps	All Versions		0001-01-01T00:00:00Z	Not Covered
An integer overflow flaw was found in pcl/pl/plfont.c:418 in pl_glyph_name in ghostscript. This issue may allow a local attacker to cause a denial of service via transforming a crafted PCL file to PDF format.	CVE-2023-38560	Low			debian:bookworm:ghostscript	All Versions		0001-01-01T00:00:00Z	Not Covered
An integer overflow flaw was found in pcl/pl/plfont.c:418 in pl_glyph_name in ghostscript. This issue may allow a local attacker to cause a denial of service via transforming a crafted PCL file to PDF format.	CVE-2023-38560	Low			debian:bookworm:libgs10-common	All Versions		0001-01-01T00:00:00Z	Not Covered
An integer overflow flaw was found in pcl/pl/plfont.c:418 in pl_glyph_name in ghostscript. This issue may allow a local attacker to cause a denial of service via transforming a crafted PCL file to PDF format.	CVE-2023-38560	Low			debian:bookworm:libgs-common	All Versions		0001-01-01T00:00:00Z	Not Covered
An integer overflow flaw was found in pcl/pl/plfont.c:418 in pl_glyph_name in ghostscript. This issue may allow a local attacker to cause a denial of service via transforming a crafted PCL file to PDF format.	CVE-2023-38560	Low			debian:bookworm:libgs10	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
stress-test master commit e4c878 was discovered to contain a FPE vulnerability via the component combine_inner at /pixman-combine-float.c.	CVE-2023-37769	Low			debian:bookworm:libpixman-1-0	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c.	CVE-2021-32256	Low			debian:bookworm:libgprofng0	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c.	CVE-2021-32256	Low			debian:bookworm:libctf-nobfd0	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c.	CVE-2021-32256	Low			debian:bookworm:libctf0	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c.	CVE-2021-32256	Low			debian:bookworm:libbinutils	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c.	CVE-2021-32256	Low			debian:bookworm:binutils-common	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c.	CVE-2021-32256	Low			debian:bookworm:binutils-x86-64-linux-gnu	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-overflow issue in demangle_type in rust-demangle.c.	CVE-2021-32256	Low			debian:bookworm:binutils	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, in some views, not all existing and sealed log messages are displayed. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31437	Low			debian:bookworm:libsystemd0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, in some views, not all existing and sealed log messages are displayed. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31437	Low			debian:bookworm:libnss-systemd	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, in some views, not all existing and sealed log messages are displayed. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31437	Low			debian:bookworm:libudev1	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, in some views, not all existing and sealed log messages are displayed. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31437	Low			debian:bookworm:libpam-systemd	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, in some views, not all existing and sealed log messages are displayed. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31437	Low			debian:bookworm:systemd-sysv	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, in some views, not all existing and sealed log messages are displayed. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31437	Low			debian:bookworm:udev	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, in some views, not all existing and sealed log messages are displayed. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31437	Low			debian:bookworm:libsystemd-shared	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, in some views, not all existing and sealed log messages are displayed. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31437	Low			debian:bookworm:systemd	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, in some views, not all existing and sealed log messages are displayed. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31437	Low			debian:bookworm:systemd-timesyncd	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify the contents of past events in a sealed log file and then adjust the file such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31439	Low			debian:bookworm:udev	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify the contents of past events in a sealed log file and then adjust the file such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31439	Low			debian:bookworm:systemd-sysv	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify the contents of past events in a sealed log file and then adjust the file such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31439	Low			debian:bookworm:libnss-systemd	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in systemd 253. An attacker can modify the contents of past events in a sealed log file and then adjust the file such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31439	Low			debian:bookworm:libsystemd0	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify the contents of past events in a sealed log file and then adjust the file such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31439	Low			debian:bookworm:systemd-timesyncd	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify the contents of past events in a sealed log file and then adjust the file such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31439	Low			debian:bookworm:libsystemd-shared	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify the contents of past events in a sealed log file and then adjust the file such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31439	Low			debian:bookworm:libpam-systemd	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify the contents of past events in a sealed log file and then adjust the file such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31439	Low			debian:bookworm:libudev1	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in systemd 253. An attacker can modify the contents of past events in a sealed log file and then adjust the file such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31439	Low			debian:bookworm:systemd	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then resume log sealing such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31438	Low			debian:bookworm:systemd-sysv	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then resume log sealing such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31438	Low			debian:bookworm:libpam-systemd	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then resume log sealing such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31438	Low			debian:bookworm:libsystemd0	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then resume log sealing such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31438	Low			debian:bookworm:libudev1	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then resume log sealing such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31438	Low			debian:bookworm:udev	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then resume log sealing such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31438	Low			debian:bookworm:systemd	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then resume log sealing such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31438	Low			debian:bookworm:libsystemd-shared	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then resume log sealing such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31438	Low			debian:bookworm:libnss-systemd	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then resume log sealing such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31438	Low			debian:bookworm:systemd-timesyncd	All Versions		0001-01-01T00:00:00Z	Not Covered
llvm-project commit a0138390 was discovered to contain a segmentation fault via the component matchAndRewriteSortOp<mlir::sparse_tensor::SortOp>(mlir::sparse_tensor::SortOp.	CVE-2023-29941	Low			debian:bookworm:libllvm15	All Versions		0001-01-01T00:00:00Z	Not Covered
llvm-project commit a0138390 was discovered to contain a segmentation fault via the component mlir::spirv::TargetEnv::TargetEnv(mlir::spirv::TargetEnvAttr).	CVE-2023-29939	Low			debian:bookworm:libllvm15	All Versions		0001-01-01T00:00:00Z	Not Covered
llvm-project commit 6c01b5c was discovered to contain a segmentation fault via the component mlir::Type::getDialect().	CVE-2023-29934	Low			debian:bookworm:libllvm15	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
llvm-project commit bd456297 was discovered to contain a segmentation fault via the component mlir::Block::getArgument.	CVE-2023-29933	Low			debian:bookworm:libllvm15	All Versions		0001-01-01T00:00:00Z	Not Covered
llvm-project commit a0138390 was discovered to contain an assertion failure at !replacements.count(op) && "operation was already replaced.	CVE-2023-29935	Low			debian:bookworm:libllvm15	All Versions		0001-01-01T00:00:00Z	Not Covered
llvm-project commit a0138390 was discovered to contain a segmentation fault via the component mlir::Type::isa<mlir::LLVM::LLVMVoidType.	CVE-2023-29942	Low			debian:bookworm:libllvm15	All Versions		0001-01-01T00:00:00Z	Not Covered
llvm-project commit fdbc55a5 was discovered to contain a segmentation fault via the component mlir::IROperand<mlir::OpOperand.	CVE-2023-29932	Low			debian:bookworm:libllvm15	All Versions		0001-01-01T00:00:00Z	Not Covered
In Shadow 4.13, it is possible to inject control characters into fields provided to the SUID program chfn (change finger). Although it is not possible to exploit this directly (e.g., adding a new user fails because \n is in the block list), it is possible to misrepresent the /etc/passwd file when viewed. Use of \r manipulations and Unicode characters to work around blocking of the : character make it possible to give the impression that a new user has been added. In other words, an adversary may be able to convince a system administrator to take the system offline (an indirect, social-engineered denial of service) by demonstrating that "cat /etc/passwd" shows a rogue user account.	CVE-2023-29383	Low			debian:bookworm:login	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
In Shadow 4.13, it is possible to inject control characters into fields provided to the SUID program chfn (change finger). Although it is not possible to exploit this directly (e.g., adding a new user fails because \n is in the block list), it is possible to misrepresent the /etc/passwd file when viewed. Use of \r manipulations and Unicode characters to work around blocking of the : character make it possible to give the impression that a new user has been added. In other words, an adversary may be able to convince a system administrator to take the system offline (an indirect, social-engineered denial of service) by demonstrating that "cat /etc/passwd" shows a rogue user account.	CVE-2023-29383	Low			debian:bookworm:passwd	All Versions		0001-01-01T00:00:00Z	Not Covered
A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf.c. This may lead to loss of availability.	CVE-2023-1972	Low			debian:bookworm:libctf-nobfd0	All Versions		0001-01-01T00:00:00Z	Not Covered
A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf.c. This may lead to loss of availability.	CVE-2023-1972	Low			debian:bookworm:libgprofng0	All Versions		0001-01-01T00:00:00Z	Not Covered
A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf.c. This may lead to loss of availability.	CVE-2023-1972	Low			debian:bookworm:libctf0	All Versions		0001-01-01T00:00:00Z	Not Covered
A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf.c. This may lead to loss of availability.	CVE-2023-1972	Low			debian:bookworm:libbinutils	All Versions		0001-01-01T00:00:00Z	Not Covered
A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf.c. This may lead to loss of availability.	CVE-2023-1972	Low			debian:bookworm:binutils-common	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf.c. This may lead to loss of availability.	CVE-2023-1972	Low			debian:bookworm:binutils	All Versions		0001-01-01T00:00:00Z	Not Covered
A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf.c. This may lead to loss of availability.	CVE-2023-1972	Low			debian:bookworm:binutils-x86-64-linux-gnu	All Versions		0001-01-01T00:00:00Z	Not Covered
LLVM a0dab4950 has a segmentation fault in mlir::outlineSingleBlockRegion. NOTE: third parties dispute this because the LLVM security policy excludes "Language front-ends ... for which a malicious input file can cause undesirable behavior."	CVE-2023-26924	Low			debian:bookworm:libllvm15	All Versions		0001-01-01T00:00:00Z	Not Covered
A flaw was found in tiffcrop, a program distributed by the libtiff package. A specially crafted tiff file can lead to an out-of-bounds read in the extractImageSection function in tools/tiffcrop.c, resulting in a denial of service and limited information disclosure. This issue affects libtiff versions 4.x.	CVE-2023-1916	Low			debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
LibTIFF version 4.0.7 is vulnerable to a heap-based buffer over-read in tif_lzw.c resulting in DoS or code execution via a crafted bmp image to tools/bmp2tiff.	CVE-2017-5563	Low			debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
An integer overflow vulnerability was found in tiftoimage function in openjpeg 2.1.2, resulting in heap buffer overflow.	CVE-2016-9580	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered
An infinite loop vulnerability in tiftoimage that results in heap buffer overflow in convert_32s_C1P1 was found in openjpeg 2.1.2.	CVE-2016-9581	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered
GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.	CVE-2022-3219	Low			debian:bookworm:gpgsm	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.	CVE-2022-3219	Low			debian:bookworm:gpg-agent	All Versions		0001-01-01T00:00:00Z	Not Covered
GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.	CVE-2022-3219	Low			debian:bookworm:gpgv	All Versions		0001-01-01T00:00:00Z	Not Covered
GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.	CVE-2022-3219	Low			debian:bookworm:gpg	All Versions		0001-01-01T00:00:00Z	Not Covered
GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.	CVE-2022-3219	Low			debian:bookworm:gpg-wks-client	All Versions		0001-01-01T00:00:00Z	Not Covered
GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.	CVE-2022-3219	Low			debian:bookworm:dirmngr	All Versions		0001-01-01T00:00:00Z	Not Covered
GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.	CVE-2022-3219	Low			debian:bookworm:gnupg-l10n	All Versions		0001-01-01T00:00:00Z	Not Covered
GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.	CVE-2022-3219	Low			debian:bookworm:gpg-wks-server	All Versions		0001-01-01T00:00:00Z	Not Covered
GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.	CVE-2022-3219	Low			debian:bookworm:gnupg-utils	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.	CVE-2022-3219	Low			debian:bookworm:gpgconf	All Versions		0001-01-01T00:00:00Z	Not Covered
GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.	CVE-2022-3219	Low			debian:bookworm:gnupg	All Versions		0001-01-01T00:00:00Z	Not Covered
The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.	CVE-2011-3389	Low			debian:bookworm:libgnutls30	All Versions		0001-01-01T00:00:00Z	Not Covered
extensions/libxt_tcp.c in iptables through 1.4.21 does not match TCP SYN+FIN packets in --syn rules, which might allow remote attackers to bypass intended firewall restrictions via crafted packets. NOTE: the CVE-2012-6638 fix makes this issue less relevant.	CVE-2012-2663	Low			debian:bookworm:libip4tc2	All Versions		0001-01-01T00:00:00Z	Not Covered
The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted file. NOTE: the vendor says "This is a Q64 issue and we do not support Q64."	CVE-2016-8678	Low			debian:bookworm:libmagickcore-6.q16-6-extra	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted file. NOTE: the vendor says "This is a Q64 issue and we do not support Q64."	CVE-2016-8678	Low			debian:bookworm:imagemagick-6-common	All Versions		0001-01-01T00:00:00Z	Not Covered
The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted file. NOTE: the vendor says "This is a Q64 issue and we do not support Q64."	CVE-2016-8678	Low			debian:bookworm:libmagickwand-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted file. NOTE: the vendor says "This is a Q64 issue and we do not support Q64."	CVE-2016-8678	Low			debian:bookworm:libmagickcore-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
NULL Pointer Access in function imagetopnm of convert.c(jp2):1289 in OpenJPEG 2.1.2. Impact is Denial of Service. Someone must open a crafted j2k file.	CVE-2016-9117	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered
Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to cause a denial of service (crash, infinite loop, or memory consumption) via (a) unspecified vectors in the (1) AVI, (2) AVS, (3) DCM, (4) EPT, (5) FITS, (6) MTV, (7) PALM, (8) RLA, and (9) TGA decoder readers; and (b) the GetImageCharacteristics function in magick/image.c, as reachable from a crafted (10) PNG, (11) JPEG, (12) BMP, or (13) TIFF file.	CVE-2008-3134	Low			debian:bookworm:libmagickcore-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to cause a denial of service (crash, infinite loop, or memory consumption) via (a) unspecified vectors in the (1) AVI, (2) AVS, (3) DCM, (4) EPT, (5) FITS, (6) MTV, (7) PALM, (8) RLA, and (9) TGA decoder readers; and (b) the GetImageCharacteristics function in magick/image.c, as reachable from a crafted (10) PNG, (11) JPEG, (12) BMP, or (13) TIFF file.	CVE-2008-3134	Low			debian:bookworm:imagemagick-6-common	All Versions		0001-01-01T00:00:00Z	Not Covered
Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to cause a denial of service (crash, infinite loop, or memory consumption) via (a) unspecified vectors in the (1) AVI, (2) AVS, (3) DCM, (4) EPT, (5) FITS, (6) MTV, (7) PALM, (8) RLA, and (9) TGA decoder readers; and (b) the GetImageCharacteristics function in magick/image.c, as reachable from a crafted (10) PNG, (11) JPEG, (12) BMP, or (13) TIFF file.	CVE-2008-3134	Low			debian:bookworm:libmagickwand-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to cause a denial of service (crash, infinite loop, or memory consumption) via (a) unspecified vectors in the (1) AVI, (2) AVS, (3) DCM, (4) EPT, (5) FITS, (6) MTV, (7) PALM, (8) RLA, and (9) TGA decoder readers; and (b) the GetImageCharacteristics function in magick/image.c, as reachable from a crafted (10) PNG, (11) JPEG, (12) BMP, or (13) TIFF file.	CVE-2008-3134	Low			debian:bookworm:libmagickcore-6.q16-6-extra	All Versions		0001-01-01T00:00:00Z	Not Covered
The (a) imagearc and (b) imagefilledarc functions in GD Graphics Library (libgd) before 2.0.35 allow attackers to cause a denial of service (CPU consumption) via a large (1) start or (2) end angle degree value.	CVE-2007-3477	Low			debian:bookworm:libwmflite-0.2-7	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The browsing feature in the server in CUPS does not filter ANSI escape sequences from shared printer names, which might allow remote attackers to execute arbitrary code via a crafted printer name.	CVE-2014-8166	Low			debian:bookworm:libcups2	All Versions		0001-01-01T00:00:00Z	Not Covered
initscripts in rPath Linux 1 sets insecure permissions for the /var/log/btmp file, which allows local users to obtain sensitive information regarding authentication attempts. NOTE: because sshd detects the insecure permissions and does not log certain events, this also prevents sshd from logging failed authentication attempts by remote attackers.	CVE-2007-5686	Low			debian:bookworm:login	All Versions		0001-01-01T00:00:00Z	Not Covered
initscripts in rPath Linux 1 sets insecure permissions for the /var/log/btmp file, which allows local users to obtain sensitive information regarding authentication attempts. NOTE: because sshd detects the insecure permissions and does not log certain events, this also prevents sshd from logging failed authentication attempts by remote attackers.	CVE-2007-5686	Low			debian:bookworm:passwd	All Versions		0001-01-01T00:00:00Z	Not Covered
The nss_parse_ciphers function in libraries/libldap/tls_m.c in OpenLDAP does not properly parse OpenSSL-style multi-keyword mode cipher strings, which might cause a weaker than intended cipher to be used and allow remote attackers to have unspecified impact via unknown vectors.	CVE-2015-3276	Low			debian:bookworm:libldap-common	All Versions		0001-01-01T00:00:00Z	Not Covered
The nss_parse_ciphers function in libraries/libldap/tls_m.c in OpenLDAP does not properly parse OpenSSL-style multi-keyword mode cipher strings, which might cause a weaker than intended cipher to be used and allow remote attackers to have unspecified impact via unknown vectors.	CVE-2015-3276	Low			debian:bookworm:libldap-2.5-0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
NULL Pointer Access in function imagetopnm of convert.c:2226(jp2) in OpenJPEG 2.1.2. Impact is Denial of Service. Someone must open a crafted j2k file.	CVE-2016-9116	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered
A design flaw in image processing software that modifies JPEG images might not modify the original EXIF thumbnail, which could lead to an information leak of potentially sensitive visual information that had been removed from the main JPEG image.	CVE-2005-0406	Low			debian:bookworm:libmagickwand-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
A design flaw in image processing software that modifies JPEG images might not modify the original EXIF thumbnail, which could lead to an information leak of potentially sensitive visual information that had been removed from the main JPEG image.	CVE-2005-0406	Low			debian:bookworm:libmagickcore-6.q16-6-extra	All Versions		0001-01-01T00:00:00Z	Not Covered
A design flaw in image processing software that modifies JPEG images might not modify the original EXIF thumbnail, which could lead to an information leak of potentially sensitive visual information that had been removed from the main JPEG image.	CVE-2005-0406	Low			debian:bookworm:imagemagick-6-common	All Versions		0001-01-01T00:00:00Z	Not Covered
A design flaw in image processing software that modifies JPEG images might not modify the original EXIF thumbnail, which could lead to an information leak of potentially sensitive visual information that had been removed from the main JPEG image.	CVE-2005-0406	Low			debian:bookworm:libmagickcore-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
_is_safe in the File::Temp module for Perl does not properly handle symlinks.	CVE-2011-4116	Low			debian:bookworm:perl	All Versions		0001-01-01T00:00:00Z	Not Covered
_is_safe in the File::Temp module for Perl does not properly handle symlinks.	CVE-2011-4116	Low			debian:bookworm:perl-base	All Versions		0001-01-01T00:00:00Z	Not Covered
_is_safe in the File::Temp module for Perl does not properly handle symlinks.	CVE-2011-4116	Low			debian:bookworm:perl-modules-5.36	All Versions		0001-01-01T00:00:00Z	Not Covered
_is_safe in the File::Temp module for Perl does not properly handle symlinks.	CVE-2011-4116	Low			debian:bookworm:libperl5.36	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Heap Buffer Over-read in function imagetotga of convert.c(jp2):942 in OpenJPEG 2.1.2. Impact is Denial of Service. Someone must open a crafted j2k file.	CVE-2016-9115	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered
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	Low			debian:bookworm:libpolkit-agent-1-0	All Versions		0001-01-01T00:00:00Z	Not Covered
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	Low			debian:bookworm:libpolkit-gobject-1-0	All Versions		0001-01-01T00:00:00Z	Not Covered
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	Low			debian:bookworm:polkitd	All Versions		0001-01-01T00:00:00Z	Not Covered
There is a NULL Pointer Access in function imagetopnm of convert.c:1943(jp2) of OpenJPEG 2.1.2. image->comps[compno].data is not assigned a value after initialization(NULL). Impact is Denial of Service.	CVE-2016-9114	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered
Array index error in gd_gif_in.c in the GD Graphics Library (libgd) before 2.0.35 allows user-assisted remote attackers to cause a denial of service (crash and heap corruption) via large color index values in crafted image data, which results in a segmentation fault.	CVE-2007-3476	Low			debian:bookworm:libwmflite-0.2-7	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
GLib 2.31.8 and earlier, when the g_str_hash function is used, computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that maintains a hash table. NOTE: this issue may be disputed by the vendor; the existence of the g_str_hash function is not a vulnerability in the library, because callers of g_hash_table_new and g_hash_table_new_full can specify an arbitrary hash function that is appropriate for the application.	CVE-2012-0039	Low			debian:bookworm:libglib2.0-0	All Versions		0001-01-01T00:00:00Z	Not Covered
There is a NULL pointer dereference in function imagetobmp of convertbmp.c:980 of OpenJPEG 2.1.2. image->comps[0].data is not assigned a value after initialization(NULL). Impact is Denial of Service.	CVE-2016-9113	Low			debian:bookworm:libopenjp2-7	All Versions		0001-01-01T00:00:00Z	Not Covered
chroot in GNU coreutils, when used with --userspec, 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-2016-2781	Low			debian:bookworm:coreutils	All Versions		0001-01-01T00:00:00Z	Not Covered
libjxl v0.5.0 is affected by a Assertion failed issue in lib/jxl/image.cc jxl::PlaneBase::PlaneBase(). When encoding a malicous GIF file using cjxl, an attacker can trigger a denial of service.	CVE-2021-36691	Low			debian:bookworm:libjxl0.7	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability classified as problematic was found in GhostPCL 9.55.0. This vulnerability affects the function chunk_free_object of the file gsmchunk.c. The manipulation with a malicious file leads to a memory corruption. The attack can be initiated remotely but requires user interaction. The exploit has been disclosed to the public as a POC and may be used. It is recommended to apply the patches to fix this issue.	CVE-2022-1350	Low			debian:bookworm:libgs10	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A vulnerability classified as problematic was found in GhostPCL 9.55.0. This vulnerability affects the function chunk_free_object of the file gsmchunk.c. The manipulation with a malicious file leads to a memory corruption. The attack can be initiated remotely but requires user interaction. The exploit has been disclosed to the public as a POC and may be used. It is recommended to apply the patches to fix this issue.	CVE-2022-1350	Low			debian:bookworm:ghostscript	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability classified as problematic was found in GhostPCL 9.55.0. This vulnerability affects the function chunk_free_object of the file gsmchunk.c. The manipulation with a malicious file leads to a memory corruption. The attack can be initiated remotely but requires user interaction. The exploit has been disclosed to the public as a POC and may be used. It is recommended to apply the patches to fix this issue.	CVE-2022-1350	Low			debian:bookworm:libgs-common	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability classified as problematic was found in GhostPCL 9.55.0. This vulnerability affects the function chunk_free_object of the file gsmchunk.c. The manipulation with a malicious file leads to a memory corruption. The attack can be initiated remotely but requires user interaction. The exploit has been disclosed to the public as a POC and may be used. It is recommended to apply the patches to fix this issue.	CVE-2022-1350	Low			debian:bookworm:libgs10-common	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:libubsan1	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:liblsan0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:libstdc++6	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:libgfortran5	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:g++-12	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:cpp-12	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:libquadmath0	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:libasan8	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:gcc-12	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:libtsan2	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:libgomp1	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:libitm1	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:libcc1-0	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:libgcc-s1	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:libatomic1	All Versions		0001-01-01T00:00:00Z	Not Covered
libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	CVE-2022-27943	Low			debian:bookworm:gcc-12-base	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability classified as problematic was found in LibTIFF 4.3.0. Affected by this vulnerability is the TIFF File Handler of tiff2ps. Opening a malicious file leads to a denial of service. The attack can be launched remotely but requires user interaction. The exploit has been disclosed to the public and may be used.	CVE-2022-1210	Low			debian:bookworm:libtiff6	All Versions		0001-01-01T00:00:00Z	Not Covered
libcaca is affected by a Divide By Zero issue via img2txt, which allows a remote malicious user to cause a Denial of Service	CVE-2022-0856	Low			debian:bookworm:libcaca0	All Versions		0001-01-01T00:00:00Z	Not Covered
A Memory Leak vulnerability exists in SQLite Project SQLite3 3.35.1 and 3.37.0 via maliciously crafted SQL Queries (made via editing the Database File), it is possible to query a record, and leak subsequent bytes of memory that extend beyond the record, which could let a malicious user obtain sensitive information. NOTE: The developer disputes this as a vulnerability stating that If you give SQLite a corrupted database file and submit a query against the database, it might read parts of the database that you did not intend or expect.	CVE-2021-45346	Low			debian:bookworm:libsqlite3-0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A heap overflow flaw was found in libpngs' pngimage.c program. This flaw allows an attacker with local network access to pass a specially crafted PNG file to the pngimage utility, causing an application to crash, leading to a denial of service.	CVE-2021-4214	Low			debian:bookworm:libpng16-16	All Versions		0001-01-01T00:00:00Z	Not Covered
A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGBTransformImage() in the MagickCore/colorspace.c may trigger undefined behavior via a crafted image file that is submitted by an attacker processed by an application using ImageMagick. The highest threat from this vulnerability is to system availability.	CVE-2021-20311	Low			debian:bookworm:libmagickcore-6.q16-6-extra	All Versions		0001-01-01T00:00:00Z	Not Covered
A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGBTransformImage() in the MagickCore/colorspace.c may trigger undefined behavior via a crafted image file that is submitted by an attacker processed by an application using ImageMagick. The highest threat from this vulnerability is to system availability.	CVE-2021-20311	Low			debian:bookworm:imagemagick-6-common	All Versions		0001-01-01T00:00:00Z	Not Covered
A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGBTransformImage() in the MagickCore/colorspace.c may trigger undefined behavior via a crafted image file that is submitted by an attacker processed by an application using ImageMagick. The highest threat from this vulnerability is to system availability.	CVE-2021-20311	Low			debian:bookworm:libmagickcore-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered
A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGBTransformImage() in the MagickCore/colorspace.c may trigger undefined behavior via a crafted image file that is submitted by an attacker processed by an application using ImageMagick. The highest threat from this vulnerability is to system availability.	CVE-2021-20311	Low			debian:bookworm:libmagickwand-6.q16-6	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in Jansson through 2.13.1. Due to a parsing error in json_loads, there's an out-of-bounds read-access bug. NOTE: the vendor reports that this only occurs when a programmer fails to follow the API specification	CVE-2020-36325	Low			debian:bookworm:libjansson4	All Versions		0001-01-01T00:00:00Z	Not Covered
libldap in certain third-party OpenLDAP packages has a certificate-validation flaw when the third-party package is asserting RFC6125 support. It considers CN even when there is a non-matching subjectAltName (SAN). This is fixed in, for example, openldap-2.4.46-10.el8 in Red Hat Enterprise Linux.	CVE-2020-15719	Low			debian:bookworm:libldap-2.5-0	All Versions		0001-01-01T00:00:00Z	Not Covered
libldap in certain third-party OpenLDAP packages has a certificate-validation flaw when the third-party package is asserting RFC6125 support. It considers CN even when there is a non-matching subjectAltName (SAN). This is fixed in, for example, openldap-2.4.46-10.el8 in Red Hat Enterprise Linux.	CVE-2020-15719	Low			debian:bookworm:libldap-common	All Versions		0001-01-01T00:00:00Z	Not Covered
nghttp2 is an implementation of the Hypertext Transfer Protocol version 2 in C. The nghttp2 library prior to version 1.61.0 keeps reading the unbounded number of HTTP/2 CONTINUATION frames even after a stream is reset to keep HPACK context in sync. This causes excessive CPU usage to decode HPACK stream. nghttp2 v1.61.0 mitigates this vulnerability by limiting the number of CONTINUATION frames it accepts per stream. There is no workaround for this vulnerability.	CVE-2024-28182	Unknown	High		debian:bookworm:libnghttp2-14	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.	CVE-2023-50868	Unknown	High		debian:bookworm:libudev1	All Versions		0001-01-01T00:00:00Z	Not Covered
The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.	CVE-2023-50868	Unknown	High		debian:bookworm:systemd-sysv	All Versions		0001-01-01T00:00:00Z	Not Covered
The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.	CVE-2023-50868	Unknown	High		debian:bookworm:udev	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.	CVE-2023-50868	Unknown	High		debian:bookworm:libsystemd0	All Versions		0001-01-01T00:00:00Z	Not Covered
The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.	CVE-2023-50868	Unknown	High		debian:bookworm:libpam-systemd	All Versions		0001-01-01T00:00:00Z	Not Covered
The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.	CVE-2023-50868	Unknown	High		debian:bookworm:libnss-systemd	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.	CVE-2023-50868	Unknown	High		debian:bookworm:libsystemd-shared	All Versions		0001-01-01T00:00:00Z	Not Covered
The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.	CVE-2023-50868	Unknown	High		debian:bookworm:systemd-timesyncd	All Versions		0001-01-01T00:00:00Z	Not Covered
The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.	CVE-2023-50868	Unknown	High		debian:bookworm:systemd	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
There exists interger overflows in libvpx in versions prior to 1.14.1.Â Calling vpx_img_alloc()Â with a large value of the d_w, d_h, or alignÂ parameter may result in integer overflows in the calculations of buffer sizes and offsets and some fields of the returned vpx_image_tÂ struct may be invalid.Â Calling vpx_img_wrap()Â with a large value of the d_w, d_h, or stride_alignÂ parameter may result in integer overflows in the calculations of buffer sizes and offsets and some fields of the returned vpx_image_tÂ struct may be invalid. We recommend upgrading to version 1.14.1 or beyond	CVE-2024-5197	Unknown			debian:bookworm:libvpx7	All Versions		0001-01-01T00:00:00Z	Not Covered
Integer overflow in libaom internal functionÂ img_alloc_helper can lead to heap buffer overflow. This function can be reached via 3 callers: * Calling aom_img_alloc() with a large value of the d_w, d_h, or align parameter may result in integer overflows in the calculations of buffer sizes and offsets and some fields of the returned aom_image_t struct may be invalid. * Calling aom_img_wrap() with a large value of the d_w, d_h, or align parameter may result in integer overflows in the calculations of buffer sizes and offsets and some fields of the returned aom_image_t struct may be invalid. * Calling aom_img_alloc_with_border() with a large value of the d_w, d_h, align, size_align, or border parameter may result in integer overflows in the calculations of buffer sizes and offsets and some fields of the returned aom_image_t struct may be invalid.	CVE-2024-5171	Unknown			debian:bookworm:libaom3	All Versions		0001-01-01T00:00:00Z	Not Covered
CVE-2024-4741	CVE-2024-4741	Unknown			debian:bookworm:libssl3	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
CVE-2024-4741	CVE-2024-4741	Unknown			debian:bookworm:openssl	All Versions		0001-01-01T00:00:00Z	Not Covered
Issue summary: Checking excessively long DSA keys or parameters may be very slow. Impact summary: Applications that use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The functions EVP_PKEY_param_check() or EVP_PKEY_public_check() perform various checks on DSA parameters. Some of those computations take a long time if the modulus (`p` parameter) is too large. Trying to use a very large modulus is slow and OpenSSL will not allow using public keys with a modulus which is over 10,000 bits in length for signature verification. However the key and parameter check functions do not limit the modulus size when performing the checks. An application that calls EVP_PKEY_param_check() or EVP_PKEY_public_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. These functions are not called by OpenSSL itself on untrusted DSA keys so only applications that directly call these functions may be vulnerable.	CVE-2024-4603	Unknown			debian:bookworm:openssl	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Also vulnerable are the OpenSSL pkey and pkeyparam command line applications when using the `-check` option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue.									

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Checking excessively long DSA keys or parameters may be very slow. Impact summary: Applications that use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The functions EVP_PKEY_param_check() or EVP_PKEY_public_check() perform various checks on DSA parameters. Some of those computations take a long time if the modulus (`p` parameter) is too large. Trying to use a very large modulus is slow and OpenSSL will not allow using public keys with a modulus which is over 10,000 bits in length for signature verification. However the key and parameter check functions do not limit the modulus size when performing the checks. An application that calls EVP_PKEY_param_check() or EVP_PKEY_public_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. These functions are not called by OpenSSL itself on untrusted DSA keys so only applications that directly call these functions may be vulnerable.	CVE-2024-4603	Unknown			debian:bookworm:libssl3	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Also vulnerable are the OpenSSL pkey and pkeyparam command line applications when using the `-check` option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue.									
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/af_stereowiden.c:120:69.	CVE-2023-51794	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/af_stereowiden.c:120:69.	CVE-2023-51794	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/af_stereowiden.c:120:69.	CVE-2023-51794	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/af_stereowiden.c:120:69.	CVE-2023-51794	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/af_stereowiden.c:120:69.	CVE-2023-51794	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/af_stereowiden.c:120:69.	CVE-2023-51794	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/af_stereowiden.c:120:69.	CVE-2023-51794	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/af_stereowiden.c:120:69.	CVE-2023-51794	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/af_stereowiden.c:120:69.	CVE-2023-51794	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
cJSON v1.7.17 was discovered to contain a segmentation violation, which can trigger through the second parameter of function cJSON_SetValuestring at cJSON.c.	CVE-2024-31755	Unknown			debian:bookworm:libcjson1	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in libde265 v1.0.12 allows a local attacker to cause a denial of service via the allocation size exceeding the maximum supported size of 0x10000000000.	CVE-2023-51792	Unknown			debian:bookworm:libde265-0	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via a floating point exception (FPE) error at libavfilter/vf_minterpolate.c:1078:60 in interpolate.	CVE-2023-51798	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via a floating point exception (FPE) error at libavfilter/vf_minterpolate.c:1078:60 in interpolate.	CVE-2023-51798	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via a floating point exception (FPE) error at libavfilter/vf_minterpolate.c:1078:60 in interpolate.	CVE-2023-51798	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via a floating point exception (FPE) error at libavfilter/vf_minterpolate.c:1078:60 in interpolate.	CVE-2023-51798	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via a floating point exception (FPE) error at libavfilter/vf_minterpolate.c:1078:60 in interpolate.	CVE-2023-51798	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via a floating point exception (FPE) error at libavfilter/vf_minterpolate.c:1078:60 in interpolate.	CVE-2023-51798	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via a floating point exception (FPE) error at libavfilter/vf_minterpolate.c:1078:60 in interpolate.	CVE-2023-51798	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via a floating point exception (FPE) error at libavfilter/vf_minterpolate.c:1078:60 in interpolate.	CVE-2023-51798	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via a floating point exception (FPE) error at libavfilter/vf_minterpolate.c:1078:60 in interpolate.	CVE-2023-51798	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showwaves.c:722:24 in showwaves_filter_frame	CVE-2023-51797	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showwaves.c:722:24 in showwaves_filter_frame	CVE-2023-51797	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showwaves.c:722:24 in showwaves_filter_frame	CVE-2023-51797	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showwaves.c:722:24 in showwaves_filter_frame	CVE-2023-51797	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showwaves.c:722:24 in showwaves_filter_frame	CVE-2023-51797	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showwaves.c:722:24 in showwaves_filter_frame	CVE-2023-51797	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showwaves.c:722:24 in showwaves_filter_frame	CVE-2023-51797	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showwaves.c:722:24 in showwaves_filter_frame	CVE-2023-51797	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showwaves.c:722:24 in showwaves_filter_frame	CVE-2023-51797	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/f_reverse.c:269:26 in areverse_request_frame.	CVE-2023-51796	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/f_reverse.c:269:26 in areverse_request_frame.	CVE-2023-51796	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/f_reverse.c:269:26 in areverse_request_frame.	CVE-2023-51796	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/f_reverse.c:269:26 in areverse_request_frame.	CVE-2023-51796	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/f_reverse.c:269:26 in areverse_request_frame.	CVE-2023-51796	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/f_reverse.c:269:26 in areverse_request_frame.	CVE-2023-51796	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/f_reverse.c:269:26 in areverse_request_frame.	CVE-2023-51796	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/f_reverse.c:269:26 in areverse_request_frame.	CVE-2023-51796	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/f_reverse.c:269:26 in areverse_request_frame.	CVE-2023-51796	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showspectrum.c:1789:52 component in showspectrumpic_request_frame	CVE-2023-51795	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showspectrum.c:1789:52 component in showspectrumpic_request_frame	CVE-2023-51795	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showspectrum.c:1789:52 component in showspectrumpic_request_frame	CVE-2023-51795	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showspectrum.c:1789:52 component in showspectrumpic_request_frame	CVE-2023-51795	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showspectrum.c:1789:52 component in showspectrumpic_request_frame	CVE-2023-51795	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showspectrum.c:1789:52 component in showspectrumpic_request_frame	CVE-2023-51795	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showspectrum.c:1789:52 component in showspectrumpic_request_frame	CVE-2023-51795	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showspectrum.c:1789:52 component in showspectrumpic_request_frame	CVE-2023-51795	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showspectrum.c:1789:52 component in showspectrumpic_request_frame	CVE-2023-51795	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavutil/imgutils.c:353:9 in image_copy_plane.	CVE-2023-51793	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavutil/imgutils.c:353:9 in image_copy_plane.	CVE-2023-51793	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavutil/imgutils.c:353:9 in image_copy_plane.	CVE-2023-51793	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavutil/imgutils.c:353:9 in image_copy_plane.	CVE-2023-51793	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavutil/imgutils.c:353:9 in image_copy_plane.	CVE-2023-51793	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavutil/imgutils.c:353:9 in image_copy_plane.	CVE-2023-51793	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavutil/imgutils.c:353:9 in image_copy_plane.	CVE-2023-51793	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavutil/imgutils.c:353:9 in image_copy_plane.	CVE-2023-51793	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavutil/imgutils.c:353:9 in image_copy_plane.	CVE-2023-51793	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulenrability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavcodec/jpegxl_parser.c in gen_alias_map.	CVE-2023-51791	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulenrability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavcodec/jpegxl_parser.c in gen_alias_map.	CVE-2023-51791	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulenrability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavcodec/jpegxl_parser.c in gen_alias_map.	CVE-2023-51791	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulenrability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavcodec/jpegxl_parser.c in gen_alias_map.	CVE-2023-51791	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulenrability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavcodec/jpegxl_parser.c in gen_alias_map.	CVE-2023-51791	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulenrability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavcodec/jpegxl_parser.c in gen_alias_map.	CVE-2023-51791	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulenrability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavcodec/jpegxl_parser.c in gen_alias_map.	CVE-2023-51791	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulenrability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavcodec/jpegxl_parser.c in gen_alias_map.	CVE-2023-51791	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulenrability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavcodec/jpegxl_parser.c in gen_alias_map.	CVE-2023-51791	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the set_encoder_id function in /fftools/ffmpeg_enc.c component.	CVE-2023-50010	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the set_encoder_id function in /fftools/ffmpeg_enc.c component.	CVE-2023-50010	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the set_encoder_id function in /fftools/ffmpeg_enc.c component.	CVE-2023-50010	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the set_encoder_id function in /fftools/ffmpeg_enc.c component.	CVE-2023-50010	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the set_encoder_id function in /fftools/ffmpeg_enc.c component.	CVE-2023-50010	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the set_encoder_id function in /fftools/ffmpeg_enc.c component.	CVE-2023-50010	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the set_encoder_id function in /fftools/ffmpeg_enc.c component.	CVE-2023-50010	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the set_encoder_id function in /fftools/ffmpeg_enc.c component.	CVE-2023-50010	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the set_encoder_id function in /fftools/ffmpeg_enc.c component.	CVE-2023-50010	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_gaussian_blur_8 function in libavfilter/edge_template.c:116:5 component.	CVE-2023-50009	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_gaussian_blur_8 function in libavfilter/edge_template.c:116:5 component.	CVE-2023-50009	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_gaussian_blur_8 function in libavfilter/edge_template.c:116:5 component.	CVE-2023-50009	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_gaussian_blur_8 function in libavfilter/edge_template.c:116:5 component.	CVE-2023-50009	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_gaussian_blur_8 function in libavfilter/edge_template.c:116:5 component.	CVE-2023-50009	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_gaussian_blur_8 function in libavfilter/edge_template.c:116:5 component.	CVE-2023-50009	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_gaussian_blur_8 function in libavfilter/edge_template.c:116:5 component.	CVE-2023-50009	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_gaussian_blur_8 function in libavfilter/edge_template.c:116:5 component.	CVE-2023-50009	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_gaussian_blur_8 function in libavfilter/edge_template.c:116:5 component.	CVE-2023-50009	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the av_malloc function in libavutil/mem.c:105:9 component.	CVE-2023-50008	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the av_malloc function in libavutil/mem.c:105:9 component.	CVE-2023-50008	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the av_malloc function in libavutil/mem.c:105:9 component.	CVE-2023-50008	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the av_malloc function in libavutil/mem.c:105:9 component.	CVE-2023-50008	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the av_malloc function in libavutil/mem.c:105:9 component.	CVE-2023-50008	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the av_malloc function in libavutil/mem.c:105:9 component.	CVE-2023-50008	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the av_malloc function in libavutil/mem.c:105:9 component.	CVE-2023-50008	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the av_malloc function in libavutil/mem.c:105:9 component.	CVE-2023-50008	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the av_malloc function in libavutil/mem.c:105:9 component.	CVE-2023-50008	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via theav_samples_set_silence function in thelibavutil/samplefmt.c:260:9 component.	CVE-2023-50007	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via theav_samples_set_silence function in thelibavutil/samplefmt.c:260:9 component.	CVE-2023-50007	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via theav_samples_set_silence function in thelibavutil/samplefmt.c:260:9 component.	CVE-2023-50007	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via theav_samples_set_silence function in thelibavutil/samplefmt.c:260:9 component.	CVE-2023-50007	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via theav_samples_set_silence function in thelibavutil/samplefmt.c:260:9 component.	CVE-2023-50007	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via theav_samples_set_silence function in thelibavutil/samplefmt.c:260:9 component.	CVE-2023-50007	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via theav_samples_set_silence function in thelibavutil/samplefmt.c:260:9 component.	CVE-2023-50007	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via theav_samples_set_silence function in thelibavutil/samplefmt.c:260:9 component.	CVE-2023-50007	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via theav_samples_set_silence function in thelibavutil/samplefmt.c:260:9 component.	CVE-2023-50007	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_bwdif_filter_intra_c function in the libavfilter/bwdifdsp.c:125:5 component.	CVE-2023-49502	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_bwdif_filter_intra_c function in the libavfilter/bwdifdsp.c:125:5 component.	CVE-2023-49502	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_bwdif_filter_intra_c function in the libavfilter/bwdifdsp.c:125:5 component.	CVE-2023-49502	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_bwdif_filter_intra_c function in the libavfilter/bwdifdsp.c:125:5 component.	CVE-2023-49502	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_bwdif_filter_intra_c function in the libavfilter/bwdifdsp.c:125:5 component.	CVE-2023-49502	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_bwdif_filter_intra_c function in the libavfilter/bwdifdsp.c:125:5 component.	CVE-2023-49502	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_bwdif_filter_intra_c function in the libavfilter/bwdifdsp.c:125:5 component.	CVE-2023-49502	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_bwdif_filter_intra_c function in the libavfilter/bwdifdsp.c:125:5 component.	CVE-2023-49502	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_bwdif_filter_intra_c function in the libavfilter/bwdifdsp.c:125:5 component.	CVE-2023-49502	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the config_eq_output function in the libavfilter/asrc_afirsrc.c:495:30 component.	CVE-2023-49501	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the config_eq_output function in the libavfilter/asrc_afirsrc.c:495:30 component.	CVE-2023-49501	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the config_eq_output function in the libavfilter/asrc_afirsrc.c:495:30 component.	CVE-2023-49501	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the config_eq_output function in the libavfilter/asrc_afirsrc.c:495:30 component.	CVE-2023-49501	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the config_eq_output function in the libavfilter/asrc_afirsrc.c:495:30 component.	CVE-2023-49501	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the config_eq_output function in the libavfilter/asrc_afirsrc.c:495:30 component.	CVE-2023-49501	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the config_eq_output function in the libavfilter/asrc_afirsrc.c:495:30 component.	CVE-2023-49501	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the config_eq_output function in the libavfilter/asrc_afirsrc.c:495:30 component.	CVE-2023-49501	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the config_eq_output function in the libavfilter/asrc_afirsrc.c:495:30 component.	CVE-2023-49501	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n5.1 to n6.1 was discovered to contain an Off-by-one Error vulnerability in libavfilter/avf_showspectrum.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	CVE-2024-31585	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n5.1 to n6.1 was discovered to contain an Off-by-one Error vulnerability in libavfilter/avf_showspectrum.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	CVE-2024-31585	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
FFmpeg version n5.1 to n6.1 was discovered to contain an Off-by-one Error vulnerability in libavfilter/avf_showspectrum.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	CVE-2024-31585	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n5.1 to n6.1 was discovered to contain an Off-by-one Error vulnerability in libavfilter/avf_showspectrum.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	CVE-2024-31585	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n5.1 to n6.1 was discovered to contain an Off-by-one Error vulnerability in libavfilter/avf_showspectrum.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	CVE-2024-31585	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n5.1 to n6.1 was discovered to contain an Off-by-one Error vulnerability in libavfilter/avf_showspectrum.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	CVE-2024-31585	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n5.1 to n6.1 was discovered to contain an Off-by-one Error vulnerability in libavfilter/avf_showspectrum.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	CVE-2024-31585	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n5.1 to n6.1 was discovered to contain an Off-by-one Error vulnerability in libavfilter/avf_showspectrum.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	CVE-2024-31585	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
FFmpeg version n5.1 to n6.1 was discovered to contain an Off-by-one Error vulnerability in libavfilter/avf_showspectrum.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	CVE-2024-31585	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain a heap buffer overflow vulnerability in the draw_block_rectangle function of libavfilter/vf_codecview.c. This vulnerability allows attackers to cause undefined behavior or a Denial of Service (DoS) via crafted input.	CVE-2024-31582	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain a heap buffer overflow vulnerability in the draw_block_rectangle function of libavfilter/vf_codecview.c. This vulnerability allows attackers to cause undefined behavior or a Denial of Service (DoS) via crafted input.	CVE-2024-31582	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain a heap buffer overflow vulnerability in the draw_block_rectangle function of libavfilter/vf_codecview.c. This vulnerability allows attackers to cause undefined behavior or a Denial of Service (DoS) via crafted input.	CVE-2024-31582	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain a heap buffer overflow vulnerability in the draw_block_rectangle function of libavfilter/vf_codecview.c. This vulnerability allows attackers to cause undefined behavior or a Denial of Service (DoS) via crafted input.	CVE-2024-31582	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain a heap buffer overflow vulnerability in the draw_block_rectangle function of libavfilter/vf_codecview.c. This vulnerability allows attackers to cause undefined behavior or a Denial of Service (DoS) via crafted input.	CVE-2024-31582	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
FFmpeg version n6.1 was discovered to contain a heap buffer overflow vulnerability in the draw_block_rectangle function of libavfilter/vf_codecview.c. This vulnerability allows attackers to cause undefined behavior or a Denial of Service (DoS) via crafted input.	CVE-2024-31582	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain a heap buffer overflow vulnerability in the draw_block_rectangle function of libavfilter/vf_codecview.c. This vulnerability allows attackers to cause undefined behavior or a Denial of Service (DoS) via crafted input.	CVE-2024-31582	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain a heap buffer overflow vulnerability in the draw_block_rectangle function of libavfilter/vf_codecview.c. This vulnerability allows attackers to cause undefined behavior or a Denial of Service (DoS) via crafted input.	CVE-2024-31582	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain a heap buffer overflow vulnerability in the draw_block_rectangle function of libavfilter/vf_codecview.c. This vulnerability allows attackers to cause undefined behavior or a Denial of Service (DoS) via crafted input.	CVE-2024-31582	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain an improper validation of array index vulnerability in libavcodec/cbs_h266_syntax_template.c. This vulnerability allows attackers to cause undefined behavior within the application.	CVE-2024-31581	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain an improper validation of array index vulnerability in libavcodec/cbs_h266_syntax_template.c. This vulnerability allows attackers to cause undefined behavior within the application.	CVE-2024-31581	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
FFmpeg version n6.1 was discovered to contain an improper validation of array index vulnerability in libavcodec/cbs_h266_syntax_template.c. This vulnerability allows attackers to cause undefined behavior within the application.	CVE-2024-31581	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain an improper validation of array index vulnerability in libavcodec/cbs_h266_syntax_template.c. This vulnerability allows attackers to cause undefined behavior within the application.	CVE-2024-31581	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain an improper validation of array index vulnerability in libavcodec/cbs_h266_syntax_template.c. This vulnerability allows attackers to cause undefined behavior within the application.	CVE-2024-31581	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain an improper validation of array index vulnerability in libavcodec/cbs_h266_syntax_template.c. This vulnerability allows attackers to cause undefined behavior within the application.	CVE-2024-31581	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain an improper validation of array index vulnerability in libavcodec/cbs_h266_syntax_template.c. This vulnerability allows attackers to cause undefined behavior within the application.	CVE-2024-31581	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain an improper validation of array index vulnerability in libavcodec/cbs_h266_syntax_template.c. This vulnerability allows attackers to cause undefined behavior within the application.	CVE-2024-31581	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1 was discovered to contain an improper validation of array index vulnerability in libavcodec/cbs_h266_syntax_template.c. This vulnerability allows attackers to cause undefined behavior within the application.	CVE-2024-31581	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
FFmpeg version n6.1.1 was discovered to contain a heap use-after-free via the av_hwframe_ctx_init function.	CVE-2024-31578	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1.1 was discovered to contain a heap use-after-free via the av_hwframe_ctx_init function.	CVE-2024-31578	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1.1 was discovered to contain a heap use-after-free via the av_hwframe_ctx_init function.	CVE-2024-31578	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1.1 was discovered to contain a heap use-after-free via the av_hwframe_ctx_init function.	CVE-2024-31578	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1.1 was discovered to contain a heap use-after-free via the av_hwframe_ctx_init function.	CVE-2024-31578	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1.1 was discovered to contain a heap use-after-free via the av_hwframe_ctx_init function.	CVE-2024-31578	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1.1 was discovered to contain a heap use-after-free via the av_hwframe_ctx_init function.	CVE-2024-31578	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1.1 was discovered to contain a heap use-after-free via the av_hwframe_ctx_init function.	CVE-2024-31578	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg version n6.1.1 was discovered to contain a heap use-after-free via the av_hwframe_ctx_init function.	CVE-2024-31578	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in FFmpeg version n6.1-3-g466799d4f5, allows a local attacker to execute arbitrary code and cause a denial of service (DoS) via the af_dialoguenhance.c:261:5 in the de_stereo component.	CVE-2023-49528	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in FFmpeg version n6.1-3-g466799d4f5, allows a local attacker to execute arbitrary code and cause a denial of service (DoS) via the af_dialoguenhance.c:261:5 in the de_stereo component.	CVE-2023-49528	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Buffer Overflow vulnerability in FFmpeg version n6.1-3-g466799d4f5, allows a local attacker to execute arbitrary code and cause a denial of service (DoS) via the af_dialoguenhance.c:261:5 in the de_stereo component.	CVE-2023-49528	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in FFmpeg version n6.1-3-g466799d4f5, allows a local attacker to execute arbitrary code and cause a denial of service (DoS) via the af_dialoguenhance.c:261:5 in the de_stereo component.	CVE-2023-49528	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in FFmpeg version n6.1-3-g466799d4f5, allows a local attacker to execute arbitrary code and cause a denial of service (DoS) via the af_dialoguenhance.c:261:5 in the de_stereo component.	CVE-2023-49528	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in FFmpeg version n6.1-3-g466799d4f5, allows a local attacker to execute arbitrary code and cause a denial of service (DoS) via the af_dialoguenhance.c:261:5 in the de_stereo component.	CVE-2023-49528	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in FFmpeg version n6.1-3-g466799d4f5, allows a local attacker to execute arbitrary code and cause a denial of service (DoS) via the af_dialoguenhance.c:261:5 in the de_stereo component.	CVE-2023-49528	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in FFmpeg version n6.1-3-g466799d4f5, allows a local attacker to execute arbitrary code and cause a denial of service (DoS) via the af_dialoguenhance.c:261:5 in the de_stereo component.	CVE-2023-49528	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
Buffer Overflow vulnerability in FFmpeg version n6.1-3-g466799d4f5, allows a local attacker to execute arbitrary code and cause a denial of service (DoS) via the af_dialoguenhance.c:261:5 in the de_stereo component.	CVE-2023-49528	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue in Academy Software Foundation openexr v.3.2.3 and before allows a local attacker to cause a denial of service (DoS) via the convert function of exrmultipart.cpp.	CVE-2024-31047	Unknown			debian:bookworm:libopenexr-3-1-30	All Versions		0001-01-01T00:00:00Z	Not Covered
Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.	CVE-2024-2511	Unknown			debian:bookworm:libssl3	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.	CVE-2024-2511	Unknown			debian:bookworm:openssl	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
LLVM before 18.1.3 generates code in which the LR register can be overwritten without data being saved to the stack, and thus there can sometimes be an exploitable error in the flow of control. This affects the ARM backend and can be demonstrated with Clang. NOTE: the vendor perspective is "we don't have strong objections for a CVE to be created ... It does seem that the likelihood of this miscompile enabling an exploit remains very low, because the miscompile resulting in this JOP gadget is such that the function is most likely to crash on most valid inputs to the function. So, if this function is covered by any testing, the miscompile is most likely to be discovered before the binary is shipped to production."	CVE-2024-31852	Unknown			debian:bookworm:libllvm15	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in Mbed TLS 3.5.x before 3.6.0. When an SSL context was reset with the mbedtls_ssl_session_reset() API, the maximum TLS version to be negotiated was not restored to the configured one. An attacker was able to prevent an Mbed TLS server from establishing any TLS 1.3 connection, potentially resulting in a Denial of Service or forced version downgrade from TLS 1.3 to TLS 1.2.	CVE-2024-28755	Unknown			debian:bookworm:libmbedcrypto7	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in Mbed TLS 2.18.0 through 2.28.x before 2.28.8 and 3.x before 3.6.0, and Mbed Crypto. The PSA Crypto API mishandles shared memory.	CVE-2024-28960	Unknown			debian:bookworm:libmbedcrypto7	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
When a protocol selection parameter option disables all protocols without adding any then the default set of protocols would remain in the allowed set due to an error in the logic for removing protocols. The below command would perform a request to curl.se with a plaintext protocol which has been explicitly disabled. curl --proto -all,-http http://curl.se The flaw is only present if the set of selected protocols disables the entire set of available protocols, in itself a command with no practical use and therefore unlikely to be encountered in real situations. The curl security team has thus assessed this to be low severity bug.	CVE-2024-2004	Unknown			debian:bookworm:libcurl3-gnutls	All Versions		0001-01-01T00:00:00Z	Not Covered
When an application tells libcurl it wants to allow HTTP/2 server push, and the amount of received headers for the push surpasses the maximum allowed limit (1000), libcurl aborts the server push. When aborting, libcurl inadvertently does not free all the previously allocated headers and instead leaks the memory. Further, this error condition fails silently and is therefore not easily detected by an application.	CVE-2024-2398	Unknown			debian:bookworm:libcurl3-gnutls	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was found in the CPython `zipfile` module affecting versions 3.12.1, 3.11.7, 3.10.13, 3.9.18, and 3.8.18 and prior. The zipfile module is vulnerable to â€œquoted-overlapâ€• zip-bombs which exploit the zip format to create a zip-bomb with a high compression ratio. The fixed versions of CPython makes the zipfile module reject zip archives which overlap entries in the archive.	CVE-2024-0450	Unknown			debian:bookworm:libpython3.11-minimal	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was found in the CPython `zipfile` module affecting versions 3.12.1, 3.11.7, 3.10.13, 3.9.18, and 3.8.18 and prior. The zipfile module is vulnerable to â€œquoted-overlapâ€• zip-bombs which exploit the zip format to create a zip-bomb with a high compression ratio. The fixed versions of CPython makes the zipfile module reject zip archives which overlap entries in the archive.	CVE-2024-0450	Unknown			debian:bookworm:libpython3.11-stdlib	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was found in the CPython `zipfile` module affecting versions 3.12.1, 3.11.7, 3.10.13, 3.9.18, and 3.8.18 and prior. The zipfile module is vulnerable to â€œquoted-overlapâ€• zip-bombs which exploit the zip format to create a zip-bomb with a high compression ratio. The fixed versions of CPython makes the zipfile module reject zip archives which overlap entries in the archive.	CVE-2024-0450	Unknown			debian:bookworm:python3.11	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was found in the CPython `zipfile` module affecting versions 3.12.1, 3.11.7, 3.10.13, 3.9.18, and 3.8.18 and prior. The zipfile module is vulnerable to â€œquoted-overlapâ€• zip-bombs which exploit the zip format to create a zip-bomb with a high compression ratio. The fixed versions of CPython makes the zipfile module reject zip archives which overlap entries in the archive.	CVE-2024-0450	Unknown			debian:bookworm:python3.11-minimal	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A flaw was found in GnuTLS. The Minerva attack is a cryptographic vulnerability that exploits deterministic behavior in systems like GnuTLS, leading to side-channel leaks. In specific scenarios, such as when using the GNUTLS_PRIVKEY_FLAG_REPRODUCIBLE flag, it can result in a noticeable step in nonce size from 513 to 512 bits, exposing a potential timing side-channel.	CVE-2024-28834	Unknown			debian:bookworm:libgnutls30	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was found in the CPython `tempfile.TemporaryDirectory` class affecting versions 3.12.1, 3.11.7, 3.10.13, 3.9.18, and 3.8.18 and prior. The tempfile.TemporaryDirectory class would dereference symlinks during cleanup of permissions-related errors. This means users which can run privileged programs are potentially able to modify permissions of files referenced by symlinks in some circumstances.	CVE-2023-6597	Unknown			debian:bookworm:libpython3.11-stdlib	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was found in the CPython `tempfile.TemporaryDirectory` class affecting versions 3.12.1, 3.11.7, 3.10.13, 3.9.18, and 3.8.18 and prior. The tempfile.TemporaryDirectory class would dereference symlinks during cleanup of permissions-related errors. This means users which can run privileged programs are potentially able to modify permissions of files referenced by symlinks in some circumstances.	CVE-2023-6597	Unknown			debian:bookworm:python3.11	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was found in the CPython `tempfile.TemporaryDirectory` class affecting versions 3.12.1, 3.11.7, 3.10.13, 3.9.18, and 3.8.18 and prior. The tempfile.TemporaryDirectory class would dereference symlinks during cleanup of permissions-related errors. This means users which can run privileged programs are potentially able to modify permissions of files referenced by symlinks in some circumstances.	CVE-2023-6597	Unknown			debian:bookworm:python3.11-minimal	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was found in the CPython `tempfile.TemporaryDirectory` class affecting versions 3.12.1, 3.11.7, 3.10.13, 3.9.18, and 3.8.18 and prior. The tempfile.TemporaryDirectory class would dereference symlinks during cleanup of permissions-related errors. This means users which can run privileged programs are potentially able to modify permissions of files referenced by symlinks in some circumstances.	CVE-2023-6597	Unknown			debian:bookworm:libpython3.11-minimal	All Versions		0001-01-01T00:00:00Z	Not Covered
A flaw has been discovered in GnuTLS where an application crash can be induced when attempting to verify a specially crafted .pem bundle using the "certtool --verify-chain" command.	CVE-2024-28835	Unknown			debian:bookworm:libgnutls30	All Versions		0001-01-01T00:00:00Z	Not Covered
A timing-based side-channel flaw was found in libgcrypt's RSA implementation. This issue may allow a remote attacker to initiate a Bleichenbacher-style attack, which can lead to the decryption of RSA ciphertexts.	CVE-2024-2236	Unknown			debian:bookworm:libgcrypt20	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/k5sealv3.c.	CVE-2024-26461	Unknown			debian:bookworm:libk5crypto3	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/k5sealv3.c.	CVE-2024-26461	Unknown			debian:bookworm:krb5-locales	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/k5sealv3.c.	CVE-2024-26461	Unknown			debian:bookworm:libgssapi-krb5-2	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/k5sealv3.c.	CVE-2024-26461	Unknown			debian:bookworm:libkrb5-3	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/k5sealv3.c.	CVE-2024-26461	Unknown			debian:bookworm:libkrb5support0	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.	CVE-2024-26458	Unknown			debian:bookworm:libkrb5-3	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.	CVE-2024-26458	Unknown			debian:bookworm:libkrb5support0	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.	CVE-2024-26458	Unknown			debian:bookworm:krb5-locales	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.	CVE-2024-26458	Unknown			debian:bookworm:libgssapi-krb5-2	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.	CVE-2024-26458	Unknown			debian:bookworm:libk5crypto3	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.	CVE-2024-26462	Unknown			debian:bookworm:libkrb5-3	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.	CVE-2024-26462	Unknown			debian:bookworm:libk5crypto3	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.	CVE-2024-26462	Unknown			debian:bookworm:libkrb5support0	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.	CVE-2024-26462	Unknown			debian:bookworm:libgssapi-krb5-2	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.	CVE-2024-26462	Unknown			debian:bookworm:krb5-locales	All Versions		0001-01-01T00:00:00Z	Not Covered
ncurses 6.4-20230610 has a NULL pointer dereference in tgetstr in tinfo/lib_termcap.c.	CVE-2023-45918	Unknown			debian:bookworm:ncurses-bin	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
ncurses 6.4-20230610 has a NULL pointer dereference in tgetstr in tinfo/lib_termcap.c.	CVE-2023-45918	Unknown			debian:bookworm:libncurses6	All Versions		0001-01-01T00:00:00Z	Not Covered
ncurses 6.4-20230610 has a NULL pointer dereference in tgetstr in tinfo/lib_termcap.c.	CVE-2023-45918	Unknown			debian:bookworm:ncurses-base	All Versions		0001-01-01T00:00:00Z	Not Covered
ncurses 6.4-20230610 has a NULL pointer dereference in tgetstr in tinfo/lib_termcap.c.	CVE-2023-45918	Unknown			debian:bookworm:libtinfo6	All Versions		0001-01-01T00:00:00Z	Not Covered
ncurses 6.4-20230610 has a NULL pointer dereference in tgetstr in tinfo/lib_termcap.c.	CVE-2023-45918	Unknown			debian:bookworm:libncursesw6	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Checking excessively long invalid RSA public keys may take a long time. Impact summary: Applications that use the function EVP_PKEY_public_check() to check RSA public keys may experience long delays. Where the key that is being checked has been obtained from an untrusted source this may lead to a Denial of Service. When function EVP_PKEY_public_check() is called on RSA public keys, a computation is done to confirm that the RSA modulus, n, is composite. For valid RSA keys, n is a product of two or more large primes and this computation completes quickly. However, if n is an overly large prime, then this computation would take a long time. An application that calls EVP_PKEY_public_check() and supplies an RSA key obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function EVP_PKEY_public_check() is not called from other OpenSSL functions however it is called from the OpenSSL pkey command line application. For that reason that application is also vulnerable if used with the '-pubin' and '-check' options on untrusted data.	CVE-2023-6237	Unknown			debian:bookworm:openssl	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue.									

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Checking excessively long invalid RSA public keys may take a long time. Impact summary: Applications that use the function EVP_PKEY_public_check() to check RSA public keys may experience long delays. Where the key that is being checked has been obtained from an untrusted source this may lead to a Denial of Service. When function EVP_PKEY_public_check() is called on RSA public keys, a computation is done to confirm that the RSA modulus, n, is composite. For valid RSA keys, n is a product of two or more large primes and this computation completes quickly. However, if n is an overly large prime, then this computation would take a long time. An application that calls EVP_PKEY_public_check() and supplies an RSA key obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function EVP_PKEY_public_check() is not called from other OpenSSL functions however it is called from the OpenSSL pkey command line application. For that reason that application is also vulnerable if used with the '-pubin' and '-check' options on untrusted data.	CVE-2023-6237	Unknown			debian:bookworm:libssl3	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue.									
FFmpeg prior to commit bf814 was discovered to contain an out of bounds read via the dist->alphabet_size variable in the read_vlc_prefix() function.	CVE-2023-46407	Unknown			debian:bookworm:libpostproc56	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg prior to commit bf814 was discovered to contain an out of bounds read via the dist->alphabet_size variable in the read_vlc_prefix() function.	CVE-2023-46407	Unknown			debian:bookworm:libavdevice59	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg prior to commit bf814 was discovered to contain an out of bounds read via the dist->alphabet_size variable in the read_vlc_prefix() function.	CVE-2023-46407	Unknown			debian:bookworm:ffmpeg	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg prior to commit bf814 was discovered to contain an out of bounds read via the dist->alphabet_size variable in the read_vlc_prefix() function.	CVE-2023-46407	Unknown			debian:bookworm:libswresample4	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg prior to commit bf814 was discovered to contain an out of bounds read via the dist->alphabet_size variable in the read_vlc_prefix() function.	CVE-2023-46407	Unknown			debian:bookworm:libavformat59	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg prior to commit bf814 was discovered to contain an out of bounds read via the dist->alphabet_size variable in the read_vlc_prefix() function.	CVE-2023-46407	Unknown			debian:bookworm:libavcodec59	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg prior to commit bf814 was discovered to contain an out of bounds read via the dist->alphabet_size variable in the read_vlc_prefix() function.	CVE-2023-46407	Unknown			debian:bookworm:libavfilter8	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg prior to commit bf814 was discovered to contain an out of bounds read via the dist->alphabet_size variable in the read_vlc_prefix() function.	CVE-2023-46407	Unknown			debian:bookworm:libavutil57	All Versions		0001-01-01T00:00:00Z	Not Covered
FFmpeg prior to commit bf814 was discovered to contain an out of bounds read via the dist->alphabet_size variable in the read_vlc_prefix() function.	CVE-2023-46407	Unknown			debian:bookworm:libswscale6	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
NSS was susceptible to a timing side-channel attack when performing RSA decryption. This attack could potentially allow an attacker to recover the private data. This vulnerability affects Firefox < 124, Firefox ESR < 115.9, and Thunderbird < 115.9.	CVE-2023-5388	Unknown			debian:bookworm:libnss3	All Versions		0001-01-01T00:00:00Z	Not Covered
Mbed TLS 3.2.x through 3.4.x before 3.5 has a Buffer Overflow that can lead to remote Code execution.	CVE-2023-45199	Unknown			debian:bookworm:libmbedcrypto7	All Versions		0001-01-01T00:00:00Z	Not Covered
CVE-2010-0928	CVE-2010-0928	Unknown			debian:bookworm:openssl			0001-01-01T00:00:00Z	Not Covered
CVE-2010-0928	CVE-2010-0928	Unknown			debian:bookworm:libssl3			0001-01-01T00:00:00Z	Not Covered