Security Export

Fri Nov 15, 2019

Exported by: admin

Package type: Docker

Component name: ui-automate-service:2019.11.15-091409-feature-kltang

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The (1) maketemp and (2) mkstemp builtin functions in GNU m4 before 1.4.11 do not quote their output when a file is created, which might allow context-dependent attackers to trigger a macro expansion, leading to unspecified use of an incorrect filename.	High	security	JFrog	debian:stretch:m4	All Versions		2019-11-14T07:53:19Z
The ReadDCMImage function in coders\dcm.c in ImageMagick 7.0.6-1 has an integer signedness error leading to excessive memory consumption via a crafted DCM file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
A flaw that allowed an attacker to corrupt memory and possibly escalate privileges was found in the mwifiex kernel module while connecting to a malicious wireless network.	High	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u3	>= 4.9.168-1+deb9u3	2019-11-14T07:52:55Z
file_copy_fallback in gio/gfile.c in GNOME GLib 2.15.0 through 2.61.1 does not properly restrict file permissions while a copy operation is in progress. Instead, default permissions are used.	High	security	JFrog	debian:stretch:glib2.0	All Versions		2019-11-14T07:52:55Z
libelf/elf_end.c in elfutils 0.173 allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact because it tries to decompress twice.	High	security	JFrog	debian:stretch:elfutils	All Versions		2019-11-14T07:52:36Z
In ImageMagick 7.0.7, a NULL pointer dereference vulnerability was found in the function saveBinaryCLProgram in magick/opencl.c because a program-lookup result is not checked, related to CacheOpenCLKernel.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:23Z
ImageMagick version 7.0.7-2 contains a memory leak in ReadYCBCRImage in coders/ycbcr.c.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:11Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In GNOME GLib 2.56.1, g_markup_parse_context_end_parse() in gmarkup.c has a NULL pointer dereference.	High	security	JFrog	debian:stretch:glib2.0	All Versions		2019-11-14T07:52:37Z
An issue was discovered in dlpar_parse_cc_property in arch/powerpc/platforms/pseries/dlpar.c in the Linux kernel through 5.1.6. There is an unchecked kstrdup of prop->name, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash).	High	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:55Z
In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function PersistPixelCache in magick/cache.c, which allows attackers to cause a denial of service (memory consumption in ReadMPCImage in coders/mpc.c) via a crafted file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
** DISPUTED ** In PostgreSQL 9.3 through 11.2, the "COPY TO/FROM PROGRAM" function allows superusers and users in the 'pg_read_server_files' group to execute arbitrary code in the context of the database's operating system user. This functionality is enabled by default and can be abused to run arbitrary operating system commands on Windows, Linux, and macOS. NOTE: Third parties claim/state this is not an issue because PostgreSQL functionality for ?COPY TO/FROM PROGRAM? is acting as intended. References state that in PostgreSQL, a superuser can execute commands as the server user without using the ?COPY FROM PROGRAM?. Furthermore, members in 'pg_read_server_files' can run commands only if either the 'pg_execute_server_program' role or superuser are granted.	High	security	JFrog	debian:stretch:postgresql-9.6	All Versions		2019-11-14T07:52:51Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root access by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic). Another contributing factor is incorrect marking of a ptrace relationship as privileged, which is exploitable through (for example) Polkit's pkexec helper with PTRACE_TRACEME. NOTE: SELinux deny_ptrace might be a usable workaround in some environments.	High	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u4	>= 4.9.168-1+deb9u4	2019-11-14T07:52:58Z
ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function PostscriptDelegateMessage in coders/ps.c.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:10Z
ImageMagick 7.0.6-6 has a large loop vulnerability in ReadWPGImage in coders/wpg.c, causing CPU exhaustion via a crafted wpg image file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
libxslt through 1.1.33 allows bypass of a protection mechanism because callers of xsltCheckRead and xsltCheckWrite permit access even upon receiving a -1 error code. xsltCheckRead can return -1 for a crafted URL that is not actually invalid and is subsequently loaded.	High	security	JFrog	debian:stretch:libxslt	All Versions		2019-11-14T07:52:52Z
In ImageMagick 7.0.6-8, the load_level function in coders/xcf.c lacks offset validation, which allows attackers to cause a denial of service (load_tile memory exhaustion) via a crafted file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:05Z
ImageMagick 7.0.6-1 has a memory exhaustion vulnerability in ReadOneJNGImage in coders\png.c.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
Integer overflow in the decode_digit function in puny_decode.c in Libidn2 before 2.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact.	High	security	JFrog	debian:stretch:libidn	All Versions		2019-11-14T07:56:07Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In coders/xbm.c in ImageMagick 7.0.6-1 Q16, a DoS in ReadXBMImage() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted XBM file, which claims large rows and columns fields in the header but does not contain sufficient backing data, is provided, the loop over the rows would consume huge CPU resources, since there is no EOF check inside the loop.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:08Z
Buffer overflow in GNU Wget 1.20.1 and earlier allows remote attackers to cause a denial-of-service (DoS) or may execute an arbitrary code via unspecified vectors.	High	security	JFrog	debian:stretch:wget	< 1.18-5+deb9u3	>= 1.18-5+deb9u3	2019-11-14T07:52:51Z
The ReadBMPImage function in coders/bmp.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted BMP file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:06Z
ImageMagick 7.0.6-5 has a memory leak vulnerability in ReadWEBPImage in coders/webp.c because memory is not freed in certain error cases, as demonstrated by VP8 errors.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:08Z
GNU Libtasn1-4.13 libtasn1-4.13 version libtasn1-4.13, libtasn1-4.12 contains a DoS, specifically CPU usage will reach 100% when running asn1Paser against the POC due to an issue in _asn1_expand_object_id(p_tree), after a long time, the program will be killed. This attack appears to be exploitable via parsing a crafted file.	High	security	JFrog	debian:stretch:libtasn1-6	All Versions		2019-11-14T07:52:36Z
ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function sixel_decode in coders/sixel.c.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
The malloc implementation in the GNU C Library (aka glibc or libc6), from version 2.24 to 2.26 on powerpc, and only in version 2.26 on i386, did not properly handle malloc calls with arguments close to SIZE_MAX and could return a pointer to a heap region that is smaller than requested, eventually leading to heap corruption.	High	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:56:20Z
ImageMagick 7.0.7-0 has a NULL Pointer Dereference in TIFFIgnoreTags in coders/tiff.c.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
An issue was discovered in the Linux kernel before 4.19.9. The USB subsystem mishandles size checks during the reading of an extra descriptor, related to __usb_get_extra_descriptor in drivers/usb/core/usb.c.	High	security	JFrog	debian:stretch:linux	< 4.9.161-1	>= 4.9.161-1	2019-11-14T07:52:44Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
Double free vulnerability in MIT Kerberos 5 (aka krb5) allows attackers to have unspecified impact via vectors involving automatic deletion of security contexts on error.	High	security	JFrog	debian:stretch:krb5	All Versions		2019-11-14T07:56:07Z
The Linux kernel before 5.1-rc5 allows page->_refcount reference count overflow, with resultant use-after-free issues, if about 140 GiB of RAM exists. This is related to fs/fuse/dev.c, fs/pipe.c, fs/splice.c, include/linux/mm.h, include/linux/pipe_fs_i.h, kernel/trace/trace.c, mm/gup.c, and mm/hugetlb.c. It can occur with FUSE requests.	High	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:53Z
In PCRE 8.41, the OP_KETRMAX feature in the match function in pcre_exec.c allows stack exhaustion (uncontrolled recursion) when processing a crafted regular expression.	High	security	JFrog	debian:stretch:pcre3	All Versions		2019-11-14T07:56:01Z
The xdr_bytes and xdr_string functions in the GNU C Library (aka glibc or libc6) 2.25 mishandle failures of buffer deserialization, which allows remote attackers to cause a denial of service (virtual memory allocation, or memory consumption if an overcommit setting is not used) via a crafted UDP packet to port 111, a related issue to CVE-2017-8779.	High	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:41:45Z
A flaw was found in the Linux kernel. A heap based buffer overflow in mwifiex_uap_parse_tail_ies function in drivers/net/wireless/marvell/mwifiex/ie.c might lead to memory corruption and possibly other consequences.	High	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u3	>= 4.9.168-1+deb9u3	2019-11-14T07:52:55Z
In ImageMagick 7.0.6-2, a memory exhaustion vulnerability was found in the function ReadPSDImage in coders/psd.c, which allows attackers to cause a denial of service.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
In ImageMagick 7.0.7-1 Q16, a memory exhaustion vulnerability was found in the function ReadTIFFImage in coders/tiff.c, which allow remote attackers to cause a denial of service via a crafted file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:19Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The cineon parsing component in ImageMagick 7.0.8-26 Q16 allows attackers to cause a denial-of-service (uncontrolled resource consumption) by crafting a Cineon image with an incorrect claimed image size. This occurs because ReadCINImage in coders/cin.c lacks a check for insufficient image data in a file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:52Z
libpng before 1.6.32 does not properly check the length of chunks against the user limit.	High	security	JFrog	debian:stretch:libpng1.6	All Versions		2019-11-14T07:52:57Z
An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.	High	security	JFrog	debian:stretch:libssh2	< 1.7.0-1+deb9u1	>= 1.7.0-1+deb9u1	2019-11-14T07:52:50Z
An issue was discovered in get_vdev_port_node_info in arch/sparc/kernel/mdesc.c in the Linux kernel through 5.1.6. There is an unchecked kstrdup_const of node_info->vdev_port.name, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash).	High	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:55Z
In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-22, an infinite loop vulnerability was found in the function ReadTXTImage in coders/txt.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted image file that is mishandled in a GetImageIndexInList call.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:30Z
runuser in util-linux allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.	High	security	JFrog	debian:stretch:util-linux	All Versions		2019-11-14T07:55:24Z
An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.	High	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:56:20Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In pppol2tp_connect, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-38159931.	High	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:37Z
An issue was discovered in the Linux kernel before 4.20. There is a race condition in smp_task_timedout() and smp_task_done() in drivers/scsi/libsas/sas_expander.c, leading to a use-after-free.	High	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:53Z
In shadow before 4.5, the newusers tool could be made to manipulate internal data structures in ways unintended by the authors. Malformed input may lead to crashes (with a buffer overflow or other memory corruption) or other unspecified behaviors. This crosses a privilege boundary in, for example, certain web-hosting environments in which a Control Panel allows an unprivileged user account to create subaccounts.	High	security	JFrog	debian:stretch:shadow	All Versions		2019-11-14T07:56:04Z
An issue where a provided address with access_ok() is not checked was discovered in i915_gem_execbuffer2_ioctl in drivers/gpu/drm/i915/i915_gem_execbuffer.c in the Linux kernel through 4.19.13. A local attacker can craft a malicious IOCTL function call to overwrite arbitrary kernel memory, resulting in a Denial of Service or privilege escalation.	High	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:46Z
systemd-tmpfiles in systemd through 237 mishandles symlinks present in non-terminal path components, which allows local users to obtain ownership of arbitrary files via vectors involving creation of a directory and a file under that directory, and later replacing that directory with a symlink. This occurs even if the fs.protected_symlinks sysctl is turned on.	High	security	JFrog	debian:stretch:systemd	All Versions		2019-11-14T07:56:22Z
ntfs_end_buffer_async_read in the ntfs.ko filesystem driver in the Linux kernel 4.15.0 allows attackers to trigger a stack-based out-of-bounds write and cause a denial of service (kernel oops or panic) or possibly have unspecified other impact via a crafted ntfs filesystem.	High	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:32Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denial of service (memory consumption) via an application that processes graphics data, as demonstrated by JavaScript code that creates many CANVAS elements for rendering by Chrome or Firefox.	High	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:53:05Z
Tools/faqwiz/move-faqwiz.sh (aka the generic FAQ wizard moving tool) in Python 2.4.5 might allow local users to overwrite arbitrary files via a symlink attack on a tmp$RANDOM.tmp temporary file. NOTE: there may not be common usage scenarios in which tmp$RANDOM.tmp is located in an untrusted directory.	High	security	JFrog	debian:stretch:python-defaults	All Versions		2019-11-14T07:55:32Z
The ReadMATImageV4 function in coders/mat.c in ImageMagick 7.0.8-7 uses an uninitialized variable, leading to memory corruption.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:33Z
systemd v233 and earlier fails to safely parse usernames starting with a numeric digit (e.g. "0day"), running the service in question with root privileges rather than the user intended.	High	security	JFrog	debian:stretch:systemd	All Versions		2019-11-14T07:56:01Z
A memory leak in the kernel_read_file function in fs/exec.c in the Linux kernel through 4.20.11 allows attackers to cause a denial of service (memory consumption) by triggering vfs_read failures.	High	security	JFrog	debian:stretch:linux	< 4.9.168-1	>= 4.9.168-1	2019-11-14T07:52:49Z
In ImageMagick 7.0.7-4 Q16, a memory leak vulnerability was found in the function ReadVIPSImage in coders/vips.c, which allows attackers to cause a denial of service (memory consumption in ResizeMagickMemory in MagickCore/memory.c) via a crafted file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
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.	High	security	JFrog	debian:stretch:tar	All Versions		2019-11-14T07:53:04Z
A vulnerability in unit_deserialize of systemd allows an attacker to supply arbitrary state across systemd re-execution via NotifyAccess. This can be used to improperly influence systemd execution and possibly lead to root privilege escalation. Affected releases are systemd versions up to and including 239.	High	security	JFrog	debian:stretch:systemd	< 232-25+deb9u10	>= 232-25+deb9u10	2019-11-14T07:52:40Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In Mercurial before 4.4.1, it is possible that a specially malformed repository can cause Git subrepositories to run arbitrary code in the form of a .git/hooks/post-update script checked into the repository. Typical use of Mercurial prevents construction of such repositories, but they can be created programmatically.	High	security	JFrog	debian:stretch:mercurial	All Versions		2019-11-14T07:56:16Z
An issue was discovered in mj2/opj_mj2_extract.c in OpenJPEG 2.3.0. The output prefix was not checked for length, which could overflow a buffer, when providing a prefix with 50 or more characters on the command line.	High	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:56:23Z
In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution.	High	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:56:17Z
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.	High	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:52:57Z
The intr function in sound/oss/msnd_pinnacle.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecified other impact by changing the value of a message queue head pointer between two kernel reads of that value, aka a "double fetch" vulnerability.	High	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:55:58Z
finish_stab in stabs.c in GNU Binutils 2.30 allows attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact, as demonstrated by an out-of-bounds write of 8 bytes. This can occur during execution of objdump.	High	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:32Z
ImageMagick 7.0.7-0 has a memory exhaustion issue in ReadSUNImage in coders/sun.c.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
Memory leak in decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file.	High	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In libexpat in Expat before 2.2.7, XML input including XML names that contain a large number of colons could make the XML parser consume a high amount of RAM and CPU resources while processing (enough to be usable for denial-of-service attacks).	High	security	JFrog	debian:stretch:expat	< 2.2.0-2+deb9u2	>= 2.2.0-2+deb9u2	2019-11-14T07:52:56Z
mpatch.c in Mercurial before 4.6.1 mishandles integer addition and subtraction, aka OVE-20180430-0002.	High	security	JFrog	debian:stretch:mercurial	All Versions		2019-11-14T07:52:32Z
In ImageMagick 7.0.7-16 Q16, a vulnerability was found in the function ReadOnePNGImage in coders/png.c, which allows attackers to cause a denial of service (ReadOneMNGImage large loop) via a crafted mng image file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z
In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heap-based buffer over-read via an attempted case-insensitive regular-expression match.	High	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:52:49Z
An issue was discovered in the hwpoison implementation in mm/memory-failure.c in the Linux kernel before 5.0.4. When soft_offline_in_use_page() runs on a thp tail page after pmd is split, an attacker can cause a denial of service (BUG).	High	security	JFrog	debian:stretch:linux	< 4.9.168-1	>= 4.9.168-1	2019-11-14T07:45:06Z
In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadSUNImage in coders/sun.c, which allows attackers to cause a denial of service.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
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.	High	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:55:56Z
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.	High	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:56:16Z
Multiple integer overflows in libwebp allows attackers to have unspecified impact via unknown vectors.	High	security	JFrog	debian:stretch:libwebp	All Versions		2019-11-14T07:55:23Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
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).	High	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:07Z
In ImageMagick 7.0.6-2, a CPU exhaustion vulnerability was found in the function ReadPDBImage in coders/pdb.c, which allows attackers to cause a denial of service.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
In coders/psd.c in ImageMagick 7.0.7-0 Q16, a DoS in ReadPSDLayersInternal() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted PSD file, which claims a large "length" field in the header but does not contain sufficient backing data, is provided, the loop over "length" would consume huge CPU resources, since there is no EOF check inside the loop.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
The ReadVIFFImage function in coders/viff.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted VIFF file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:07Z
An issue was discovered in the Linux kernel before 5.0.7. A NULL pointer dereference can occur when megasas_create_frame_pool() fails in megasas_alloc_cmds() in drivers/scsi/megaraid/megaraid_sas_base.c. This causes a Denial of Service, related to a use-after-free.	High	security	JFrog	debian:stretch:linux	< 4.9.168-1	>= 4.9.168-1	2019-11-14T07:52:53Z
In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
In ImageMagick 7.0.7-12 Q16, a large loop vulnerability was found in the function ExtractPostscript in coders/wpg.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted wpg image file that triggers a ReadWPGImage call.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:16Z
BZ2_decompress in decompress.c in bzip2 through 1.0.6 has an out-of-bounds write when there are many selectors.	High	security	JFrog	debian:stretch:bzip2	All Versions		2019-11-14T07:52:56Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In coders/ps.c in ImageMagick 7.0.7-0 Q16, a DoS in ReadPSImage() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted PSD file, which claims a large "extent" field in the header but does not contain sufficient backing data, is provided, the loop over "length" would consume huge CPU resources, since there is no EOF check inside the loop.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:08Z
Unspecified vulnerability in GNU m4 before 1.4.11 might allow context-dependent attackers to execute arbitrary code, related to improper handling of filenames specified with the -F option. NOTE: it is not clear when this issue crosses privilege boundaries.	High	security	JFrog	debian:stretch:m4	All Versions		2019-11-14T07:55:10Z
The cr_parser_parse_selector_core function in cr-parser.c in libcroco 0.6.12 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted CSS file.	High	security	JFrog	debian:stretch:libcroco	All Versions		2019-11-14T07:55:57Z
ntfs_attr_find in the ntfs.ko filesystem driver in the Linux kernel 4.15.0 allows attackers to trigger a stack-based out-of-bounds write and cause a denial of service (kernel oops or panic) or possibly have unspecified other impact via a crafted ntfs filesystem.	High	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:32Z
The ReadOneLayer function in coders/xcf.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:07Z
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.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:36Z
The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Windows, (4) Cisco products, and probably other operating systems allows remote attackers to cause a denial of service (connection queue exhaustion) via multiple vectors that manipulate information in the TCP state table, as demonstrated by sockstress.	High	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:55:33Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
An error when processing the EXIF_IFD_INTEROPERABILITY and EXIF_IFD_EXIF tags within libexif version 0.6.21 can be exploited to exhaust available CPU resources.	High	security	JFrog	debian:stretch:libexif	All Versions		2019-11-14T07:52:45Z
In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-22, an infinite loop vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted MIFF image file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:30Z
ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function sixel_output_create in coders/sixel.c.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:10Z
In OpenJPEG 2.3.0, a stack-based buffer overflow was discovered in the pgxtovolume function in jp3d/convert.c. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service or possibly remote code execution.	High	security	JFrog	debian:stretch:openjpeg2	< 2.1.2-1.1+deb9u3	>= 2.1.2-1.1+deb9u3	2019-11-14T07:56:16Z
plugins/preauth/pkinit/pkinit_crypto_openssl.c in MIT Kerberos 5 (aka krb5) through 1.15.2 mishandles Distinguished Name (DN) fields, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) in situations involving untrusted X.509 data, related to the get_matching_data and X509_NAME_oneline_ex functions. NOTE: this has security relevance only in use cases outside of the MIT Kerberos distribution, e.g., the use of get_matching_data in KDC certauth plugin code that is specific to Red Hat.	High	security	JFrog	debian:stretch:krb5	All Versions		2019-11-14T07:56:14Z
Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff.	High	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u3	>= 4.9.168-1+deb9u3	2019-11-14T07:52:56Z
An issue was discovered in rds_tcp_kill_sock in net/rds/tcp.c in the Linux kernel before 5.0.8. There is a race condition leading to a use-after-free, related to net namespace cleanup.	High	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u3	>= 4.9.168-1+deb9u3	2019-11-14T07:52:53Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
SQLite3 from 3.6.0 to and including 3.27.2 is vulnerable to heap out-of-bound read in the rtreenode() function when handling invalid rtree tables.	High	security	JFrog	debian:stretch:sqlite3	All Versions		2019-11-14T07:52:55Z
The WritePixelCachePixels function in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (CPU consumption) via a crafted file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:05Z
In ImageMagick 7.0.7-12 Q16, an infinite loop vulnerability was found in the function ReadPSDChannelZip in coders/psd.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted psd image file.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:16Z
In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadMPCImage in coders/mpc.c, which allows attackers to cause a denial of service.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
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.	High	security	JFrog	debian:stretch:libwmf	All Versions		2019-11-14T07:54:50Z
ImageMagick 7.0.7-12 Q16, a CPU exhaustion vulnerability was found in the function ReadDDSInfo in coders/dds.c, which allows attackers to cause a denial of service.	High	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:18Z
** DISPUTED ** An issue was discovered in the MPT3COMMAND case in _ctl_ioctl_main in drivers/scsi/mpt3sas/mpt3sas_ctl.c in the Linux kernel through 5.1.5. It allows local users to cause a denial of service or possibly have unspecified other impact by changing the value of ioc_number between two kernel reads of that value, aka a "double fetch" vulnerability. NOTE: a third party reports that this is unexploitable because the doubly fetched value is not used.	High	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:55Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In /drivers/isdn/i4l/isdn_net.c: A user-controlled buffer is copied into a local buffer of constant size using strcpy without a length check which can cause a buffer overflow. This affects the Linux kernel 4.9-stable tree, 4.12-stable tree, 3.18-stable tree, and 4.4-stable tree.	High	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:56:05Z
The TIFFFdOpen function in tif_unix.c in LibTIFF 4.0.10 has a memory leak, as demonstrated by pal2rgb.	Medium	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:52:45Z
The snd_compr_tstamp function in sound/core/compress_offload.c in the Linux kernel through 4.7, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not properly initialize a timestamp data structure, which allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28770164 and Qualcomm internal bug CR568717.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:55:48Z
In the GNU C Library (aka glibc or libc6) through 2.28, the getaddrinfo function would successfully parse a string that contained an IPv4 address followed by whitespace and arbitrary characters, which could lead applications to incorrectly assume that it had parsed a valid string, without the possibility of embedded HTTP headers or other potentially dangerous substrings.	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:52:46Z
In ImageMagick before 7.0.8-25, a memory leak exists in WriteDIBImage in coders/dib.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:47Z
The _TIFFmalloc function in tif_unix.c in LibTIFF 4.0.3 does not reject a zero size, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted TIFF image that is mishandled by the TIFFWriteScanline function in tif_write.c, as demonstrated by tiffdither.	Medium	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:53:20Z
The pop_fail_stack function in the GNU C Library (aka glibc or libc6) allows context-dependent attackers to cause a denial of service (assertion failure and application crash) via vectors related to extended regular expression processing.	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:55:48Z
The KVM implementation in the Linux kernel through 4.20.5 has a Use-after-Free.	Medium	security	JFrog	debian:stretch:linux	< 4.9.161-1	>= 4.9.161-1	2019-11-14T07:52:47Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is a heap-based buffer overflow in _bfd_archive_64_bit_slurp_armap in archive64.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:49Z
The print_gnu_property_note function in readelf.c in GNU Binutils 2.29.1 does not have integer-overflow protection on 32-bit platforms, which allows remote attackers to cause a denial of service (segmentation violation and application crash) or possibly have unspecified other impact via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:15Z
An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an out-of-bounds read leading to a SEGV in bfd_getl32 in libbfd.c, when called from pex64_get_runtime_function in pei-x86_64.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:49Z
An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the query string after a ? character) followed by an HTTP header or a Redis command.	Medium	security	JFrog	debian:stretch:python2.7	All Versions		2019-11-14T07:52:50Z
Stack-based buffer overflow in the pcre32_copy_substring function in pcre_get.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (WRITE of size 268) or possibly have unspecified other impact via a crafted file.	Medium	security	JFrog	debian:stretch:pcre3	All Versions		2019-11-14T07:55:50Z
The bfd_make_section_with_flags function in section.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause a NULL dereference via a crafted file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:04Z
The _bfd_coff_read_string_table function in coffgen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not properly validate the size of the external string table, which allows remote attackers to cause a denial of service (excessive memory consumption, or heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted COFF binary.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:15Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
A flaw was found in libssh2 before 1.8.1. A server could send a multiple keyboard interactive response messages whose total length are greater than unsigned char max characters. This value is used as an index to copy memory causing in an out of bounds memory write error.	Medium	security	JFrog	debian:stretch:libssh2	< 1.7.0-1+deb9u1	>= 1.7.0-1+deb9u1	2019-11-14T07:52:50Z
In SQLite 3.27.2, running fts5 prefix queries inside a transaction could trigger a heap-based buffer over-read in fts5HashEntrySort in sqlite3.c, which may lead to an information leak. This is related to ext/fts5/fts5_hash.c.	Medium	security	JFrog	debian:stretch:sqlite3	All Versions		2019-11-14T07:52:51Z
In ImageMagick 7.0.8-36 Q16, there is a memory leak in the function SVGKeyValuePairs of coders/svg.c, which allows an attacker to cause a denial of service via a crafted image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:51Z
SQLite before 3.25.3, when the FTS3 extension is enabled, encounters an integer overflow (and resultant buffer overflow) for FTS3 queries in a "merge" operation that occurs after crafted changes to FTS3 shadow tables, allowing remote attackers to execute arbitrary code by leveraging the ability to run arbitrary SQL statements (such as in certain WebSQL use cases). This is a different vulnerability than CVE-2018-20346.	Medium	security	JFrog	debian:stretch:sqlite3	All Versions		2019-11-14T07:52:51Z
bfd_get_debug_link_info_1 in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to bfd_getl32.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
dwarf1.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles pointers, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file, related to parse_die and parse_line_table, as demonstrated by a parse_die heap-based buffer over-read.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
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.	Medium	security	JFrog	debian:stretch:cairo	All Versions		2019-11-14T07:52:46Z
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.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:54:41Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	Medium	security	JFrog	debian:stretch:mariadb-10.1	< 10.1.38-0+deb9u1	>= 10.1.38-0+deb9u1	2019-11-14T07:52:47Z
ImageMagick 7.0.7-2 has a memory leak in ReadSGIImage in coders/sgi.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:11Z
In ImageMagick before 7.0.8-25, a memory leak exists in WritePSDChannel in coders/psd.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:47Z
The ProcessMSLScript function in coders/msl.c in ImageMagick before 6.9.9-5 and 7.x before 7.0.6-5 allows remote attackers to cause a denial of service (memory leak) via a crafted file, related to the WriteMSLImage function.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
do_core_note in readelf.c in libmagic.a in file 5.35 allows remote attackers to cause a denial of service (stack corruption and application crash) or possibly have unspecified other impact.	Medium	security	JFrog	debian:stretch:file	All Versions		2019-11-14T07:52:49Z
elfcomm.c in readelf in GNU Binutils 2.29 allows remote attackers to cause a denial of service (excessive memory allocation) or possibly have unspecified other impact via a crafted ELF file that triggers a "buffer overflow on fuzzed archive header," related to an uninitialized variable, an improper conditional jump, and the get_archive_member_name, process_archive_index_and_symbols, and setup_archive functions.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:14Z
In the GNU C Library (aka glibc or libc6) before 2.28, parse_reg_exp in posix/regcomp.c misparses alternatives, which allows attackers to cause a denial of service (assertion failure and application exit) or trigger an incorrect result by attempting a regular-expression match.	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:52:49Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The read_symbol_stabs_debugging_info function in rddbg.c in GNU Binutils 2.29 and earlier allows remote attackers to cause an out of bounds heap read via a crafted binary file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:04Z
In the Linux kernel before 4.20.14, expand_downwards in mm/mmap.c lacks a check for the mmap minimum address, which makes it easier for attackers to exploit kernel NULL pointer dereferences on non-SMAP platforms. This is related to a capability check for the wrong task.	Medium	security	JFrog	debian:stretch:linux	< 4.9.168-1	>= 4.9.168-1	2019-11-14T07:52:50Z
coffgen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not validate the symbol count, which allows remote attackers to cause a denial of service (integer overflow and application crash, or excessive memory allocation) or possibly have unspecified other impact via a crafted PE file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:15Z
An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit status message and no payload are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	Medium	security	JFrog	debian:stretch:libssh2	< 1.7.0-1+deb9u1	>= 1.7.0-1+deb9u1	2019-11-14T07:52:50Z
The regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (application crash) via a regular expression containing adjacent bounded repetitions that bypass the intended RE_DUP_MAX limitation, as demonstrated by a {10,}{10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for ProFTPD, related to a "RE_DUP_MAX overflow."	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:54:42Z
An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the path component of a URL that lacks a ? character) followed by an HTTP header or a Redis command. This is similar to the CVE-2019-9740 query string issue.	Medium	security	JFrog	debian:stretch:python2.7	All Versions		2019-11-14T07:52:50Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
nm.c and objdump.c in GNU Binutils 2.29.1 mishandle certain global symbols, which allows remote attackers to cause a denial of service (_bfd_elf_get_symbol_version_string buffer over-read and application crash) or possibly have unspecified other impact via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:16Z
It was discovered in gnutls before version 3.6.7 upstream that there is an uninitialized pointer access in gnutls versions 3.6.3 or later which can be triggered by certain post-handshake messages.	Medium	security	JFrog	debian:stretch:gnutls28	All Versions		2019-11-14T07:52:51Z
The _bfd_vms_slurp_egsd function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an arbitrary memory read via a crafted vms alpha file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:04Z
The _bfd_xcoff_read_ar_hdr function in bfd/coff-rs6000.c and bfd/coff64-rs6000.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds stack read via a crafted COFF image file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:04Z
A flaw was found in the Linux kernel's vfio interface implementation that permits violation of the user's locked memory limit. If a device is bound to a vfio driver, such as vfio-pci, and the local attacker is administratively granted ownership of the device, it may cause a system memory exhaustion and thus a denial of service (DoS). Versions 3.10, 4.14 and 4.18 are vulnerable.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:51Z
The agroot() function in cgraph\obj.c in libcgraph.a in Graphviz 2.39.20160612.1140 has a NULL pointer dereference, as demonstrated by graphml2gv.	Medium	security	JFrog	debian:stretch:graphviz	All Versions		2019-11-14T07:52:52Z
In LibTIFF 4.0.9, there is a heap-based buffer over-read in the function PackBitsEncode in tif_packbits.c.	Medium	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:56:17Z
Info-ZIP UnZip 6.0 mishandles the overlapping of files inside a ZIP container, leading to denial of service (resource consumption), aka a "better zip bomb" issue.	Medium	security	JFrog	debian:stretch:unzip	All Versions		2019-11-14T07:52:57Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
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.	Medium	security	JFrog	debian:stretch:cups	All Versions		2019-11-14T07:54:45Z
In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadPGXImage in coders/pgx.c, which allows attackers to cause a denial of service via a crafted PGX image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z
jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.	Medium	security	JFrog	debian:stretch:jquery	< 3.1.1-2+deb9u1	>= 3.1.1-2+deb9u1	2019-11-14T07:52:52Z
The Siemens R3964 line discipline driver in drivers/tty/n_r3964.c in the Linux kernel before 5.0.8 has multiple race conditions.	Medium	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u3	>= 4.9.168-1+deb9u3	2019-11-14T07:52:53Z
In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadXPMImage in coders/xpm.c, which allows attackers to cause a denial of service via a crafted XPM image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z
It was discovered that a systemd service that uses DynamicUser property can create a SUID/SGID binary that would be allowed to run as the transient service UID/GID even after the service is terminated. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the UID/GID will be recycled.	Medium	security	JFrog	debian:stretch:systemd	All Versions		2019-11-14T07:52:53Z
In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service via a crafted MAT image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z
The htmlParseTryOrFinish function in HTMLparser.c in libxml2 2.9.4 allows attackers to cause a denial of service (buffer over-read) or information disclosure.	Medium	security	JFrog	debian:stretch:libxml2	All Versions		2019-11-14T07:55:55Z
In ImageMagick 7.0.7-17 Q16, there is a Memory Leak in ReadPWPImage in coders/pwp.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
Integer overflow in SQLite via WebSQL in Google Chrome prior to 74.0.3729.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	Medium	security	JFrog	debian:stretch:sqlite3	All Versions		2019-11-14T07:52:53Z
In ImageMagick 7.0.6-6, a memory exhaustion vulnerability was found in the function ReadTIFFImage, which allows attackers to cause a denial of service.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:53Z
ImageMagick 7.0.7-17 Q16 x86_64 has memory leaks in coders/msl.c, related to MSLPopImage and ProcessMSLScript, and associated with mishandling of MSLPushImage calls.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z
Microarchitectural Load Port Data Sampling (MLPDS): Load ports on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf	Medium	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u2	>= 4.9.168-1+deb9u2	2019-11-14T07:52:53Z
systemd 242 changes the VT1 mode upon a logout, which allows attackers to read cleartext passwords in certain circumstances, such as watching a shutdown, or using Ctrl-Alt-F1 and Ctrl-Alt-F2. This occurs because the KDGKBMODE (aka current keyboard mode) check is mishandled.	Medium	security	JFrog	debian:stretch:systemd	All Versions		2019-11-14T07:52:53Z
A NULL pointer dereference in the function ReadPANGOImage in coders/pango.c and the function ReadVIDImage in coders/vid.c in ImageMagick 7.0.8-34 allows remote attackers to cause a denial of service via a crafted image.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:56Z
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).	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:52:56Z
GNU Binutils 2017-04-03 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash), related to the process_mips_specific function in readelf.c, via a crafted ELF file that triggers a large memory-allocation attempt.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:55Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In the Linux kernel before 5.2.3, set_geometry in drivers/block/floppy.c does not validate the sect and head fields, as demonstrated by an integer overflow and out-of-bounds read. It can be triggered by an unprivileged local user when a floppy disk has been inserted. NOTE: QEMU creates the floppy device by default.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:58Z
OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.	Medium	security	JFrog	debian:stretch:openssh	All Versions		2019-11-14T07:54:56Z
In ImageMagick 7.0.7-17 Q16, there are memory leaks in ReadPATTERNImage in coders/pattern.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:18Z
** DISPUTED ** An issue was discovered in con_insert_unipair in drivers/tty/vt/consolemap.c in the Linux kernel through 5.1.5. There is a memory leak in a certain case of an ENOMEM outcome of kmalloc. NOTE: This id is disputed as not being an issue.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:55Z
In OpenJPEG 2.3.0, there is an integer overflow caused by an out-of-bounds left shift in the opj_j2k_setup_encoder function (openjp2/j2k.c). Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file.	Medium	security	JFrog	debian:stretch:openjpeg2	< 2.1.2-1.1+deb9u3	>= 2.1.2-1.1+deb9u3	2019-11-14T07:56:18Z
** DISPUTED ** An issue was discovered in sunxi_divs_clk_setup in drivers/clk/sunxi/clk-sunxi.c in the Linux kernel through 5.1.5. There is an unchecked kstrndup of derived_name, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). NOTE: This id is disputed as not being an issue because ?The memory allocation that was not checked is part of a code that only runs at boot time, before user processes are started. Therefore, there is no possibility for an unprivileged user to control it, and no denial of service.?.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:55Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
When using gdImageCreateFromXbm() function of PHP gd extension in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6, it is possible to supply data that will cause the function to use the value of uninitialized variable. This may lead to disclosing contents of the stack that has been left there by previous code.	Medium	security	JFrog	debian:stretch:libgd2	All Versions		2019-11-14T07:52:55Z
GNU Binutils 2.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to MIPS GOT mishandling in the process_mips_specific function in readelf.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:55Z
The elf_read_notesfunction in bfd/elf.c in GNU Binutils 2.29 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:04Z
ImageMagick 7.0.7-22 Q16 has memory leaks in the ReadDCMImage function in coders/dcm.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:19Z
Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e.	Medium	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u3	>= 4.9.168-1+deb9u3	2019-11-14T07:52:56Z
In ImageMagick 7.0.6-3, a missing check for multidimensional data was found in coders/mat.c, leading to a memory leak in the function ReadImage in MagickCore/constitute.c, which allows attackers to cause a denial of service.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
systemd-tmpfiles in systemd before 237 attempts to support ownership/permission changes on hardlinked files even if the fs.protected_hardlinks sysctl is turned off, which allows local users to bypass intended access restrictions via vectors involving a hard link to a file for which the user lacks write access, as demonstrated by changing the ownership of the /etc/passwd file.	Medium	security	JFrog	debian:stretch:systemd	All Versions		2019-11-14T07:56:20Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The keyfile settings backend in GNOME GLib (aka glib2.0) before 2.60.0 creates directories using g_file_make_directory_with_parents (kfsb->dir, NULL, NULL) and files using g_file_replace_contents (kfsb->file, contents, length, NULL, FALSE, G_FILE_CREATE_REPLACE_DESTINATION, NULL, NULL, NULL). Consequently, it does not properly restrict directory (and file) permissions. Instead, for directories, 0777 permissions are used; for files, default file permissions are used. This is similar to CVE-2019-12450.	Medium	security	JFrog	debian:stretch:glib2.0	All Versions		2019-11-14T07:52:56Z
GNU Binutils 2.28 allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file with many program headers, related to the get_program_headers function in readelf.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:55Z
In ImageMagick 7.0.6-10, a NULL Pointer Dereference issue is present in the ReadCUTImage function in coders/cut.c that could allow an attacker to cause a Denial of Service (in the QueueAuthenticPixelCacheNexus function within the MagickCore/cache.c file) by submitting a malformed image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:05Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
Python 2.7.14 is vulnerable to a Heap-Buffer-Overflow as well as a Heap-Use-After-Free. Python versions prior to 2.7.14 may also be vulnerable and it appears that Python 2.7.17 and prior may also be vulnerable however this has not been confirmed. The vulnerability lies when multiply threads are handling large amounts of data. In both cases there is essentially a race condition that occurs. For the Heap-Buffer-Overflow, Thread 2 is creating the size for a buffer, but Thread1 is already writing to the buffer without knowing how much to write. So when a large amount of data is being processed, it is very easy to cause memory corruption using a Heap-Buffer-Overflow. As for the Use-After-Free, Thread3->Malloc->Thread1->Free's->Thread2-Re-uses-Free'd Memory. The PSRT has stated that this is not a security vulnerability due to the fact that the attacker must be able to run code, however in some situations, such as function as a service, this vulnerability can potentially be used by an attacker to violate a trust boundary, as such the DWF feels this issue deserves a CVE.	Medium	security	JFrog	debian:stretch:python2.7	All Versions		2019-11-14T07:56:20Z
ImageMagick 7.0.8-34 has a "use of uninitialized value" vulnerability in the ReadPANGOImage function in coders/pango.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:56Z
An improper computation of p_tx0, p_tx1, p_ty0 and p_ty1 in the function opj_get_encoding_parameters in openjp2/pi.c in OpenJPEG through 2.3.0 can lead to an integer overflow.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:52:56Z
The elf_parse_notes function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (out-of-bounds read and segmentation violation) via a note with a large alignment.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:21Z
In numbers.c in libxslt 1.1.33, a type holding grouping characters of an xsl:number instruction was too narrow and an invalid character/length combination could be passed to xsltNumberFormatDecimal, leading to a read of uninitialized stack data.	Medium	security	JFrog	debian:stretch:libxslt	All Versions		2019-11-14T07:52:56Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow in MagickCore/fourier.c in ComplexImage.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
ImageMagick 7.0.6-2 has a memory leak vulnerability in WritePICTImage in coders/pict.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:05Z
In SQLite through 3.22.0, databases whose schema is corrupted using a CREATE TABLE AS statement could cause a NULL pointer dereference, related to build.c and prepare.c.	Medium	security	JFrog	debian:stretch:sqlite3	All Versions		2019-11-14T07:56:22Z
ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/threshold.c in AdaptiveThresholdImage because a height of zero is mishandled.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/statistic.c in EvaluateImages because of mishandling rows.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
A double free exists in the another_hunk function in pch.c in GNU patch through 2.7.6.	Medium	security	JFrog	debian:stretch:patch	All Versions		2019-11-14T07:56:22Z
ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of mishandling the NoSuchImage error in CLIListOperatorImages in MagickWand/operation.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
ImageMagick 7.0.8-54 Q16 allows Division by Zero in RemoveDuplicateLayers in MagickCore/layer.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection loss) to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such as BGP.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:55:12Z
In OpenEXR 2.2.0, an invalid read of size 2 in the hufDecode function in ImfHuf.cpp could cause the application to crash.	Medium	security	JFrog	debian:stretch:openexr	All Versions		2019-11-14T07:55:56Z
An issue was discovered in ImageMagick 7.0.7. The MogrifyImageList function in MagickWand/mogrify.c allows attackers to cause a denial of service (assertion failure and application exit in ReplaceImageInList) via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:22Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
GNU Libc current is affected by: Re-mapping current loaded libray 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.	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:52:57Z
http.cookiejar.DefaultPolicy.domain_return_ok in Lib/http/cookiejar.py in Python before 3.7.3 does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g., pythonicexample.com to steal cookies for example.com). When a program uses http.cookiejar.DefaultPolicy and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker. This affects 2.x through 2.7.16, 3.x before 3.4.10, 3.5.x before 3.5.7, 3.6.x before 3.6.9, and 3.7.x before 3.7.3.	Medium	security	JFrog	debian:stretch:python2.7	All Versions		2019-11-14T07:52:57Z
In parse_hid_report_descriptor in drivers/input/tablet/gtco.c in the Linux kernel through 5.2.1, a malicious USB device can send an HID report that triggers an out-of-bounds write during generation of debugging messages.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:58Z
In OpenEXR 2.2.0, a crafted image causes a heap-based buffer over-read in the hufDecode function in IlmImf/ImfHuf.cpp during exrmaketiled execution; it may result in denial of service or possibly unspecified other impact.	Medium	security	JFrog	debian:stretch:openexr	All Versions		2019-11-14T07:56:05Z
An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.32. simple_object_elf_match in simple-object-elf.c does not check for a zero shstrndx value, leading to an integer overflow and resultant heap-based buffer overflow.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:58Z
GNU binutils gold gold v1.11-v1.16 (GNU binutils v2.21-v2.31.1) is affected by: Improper Input Validation, Signed/Unsigned Comparison, Out-of-bounds Read. The impact is: Denial of service. The component is: gold/fileread.cc:497, elfcpp/elfcpp_file.h:644. The attack vector is: An ELF file with an invalid e_shoff header field must be opened.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:58Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/statistic.c in EvaluateImages because of mishandling columns.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
In ImageMagick 7.0.6-8, a memory leak vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service (memory consumption in NewLinkedList in MagickCore/linked-list.c) via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:05Z
In libgraphite2 in graphite2 1.3.11, a NULL pointer dereference vulnerability was found in Segment.cpp during a dumbRendering operation, which may allow attackers to cause a denial of service or possibly have unspecified other impact via a crafted .ttf file.	Medium	security	JFrog	debian:stretch:graphite2	All Versions		2019-11-14T07:56:23Z
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	Medium	security	JFrog	debian:stretch:mariadb-10.1	All Versions		2019-11-14T07:52:58Z
In ImageMagick 7.0.6-6, a memory leak vulnerability was found in the function formatIPTC in coders/meta.c, which allows attackers to cause a denial of service (WriteMETAImage memory consumption) via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:05Z
Mercurial version 4.5 and earlier contains a Incorrect Access Control (CWE-285) vulnerability in Protocol server that can result in Unauthorized data access. This attack appear to be exploitable via network connectivity. This vulnerability appears to have been fixed in 4.5.1.	Medium	security	JFrog	debian:stretch:mercurial	All Versions		2019-11-14T07:56:23Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The bmp_read_info_header function in bin/jp2/convertbmp.c in OpenJPEG 2.2.0 does not reject headers with a zero biBitCount, which allows remote attackers to cause a denial of service (memory allocation failure) in the opj_image_create function in lib/openjp2/image.c, related to the opj_aligned_alloc_n function in opj_malloc.c.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:56:05Z
Null Pointer Dereference in the IdentifyImage function in MagickCore/identify.c in ImageMagick through 7.0.6-10 allows an attacker to perform denial of service by sending a crafted image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:05Z
Python 2.7 before 3.4 only uses the last eight bits of the prefix to randomize hash values, which causes it to compute hash values without restricting the ability to trigger hash collisions predictably and makes it easier for context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that maintains a hash table. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1150.	Medium	security	JFrog	debian:stretch:python2.7	All Versions		2019-11-14T07:53:38Z
Linux Linux kernel version at least v4.8 onwards, probably well before contains a Insufficient input validation vulnerability in bnx2x network card driver that can result in DoS: Network card firmware assertion takes card off-line. This attack appear to be exploitable via An attacker on a must pass a very large, specially crafted packet to the bnx2x card. This can be done from an untrusted guest VM..	Medium	security	JFrog	debian:stretch:linux	< 4.9.161-1	>= 4.9.161-1	2019-11-14T07:56:23Z
An issue was discovered in ImageMagick 7.0.7. A memory leak vulnerability was found in the function WriteGIFImage in coders/gif.c, which allow remote attackers to cause a denial of service via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:24Z
The swap_std_reloc_in function in aoutx.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (aout_32_swap_std_reloc_out NULL pointer dereference and application crash) via a crafted ELF file, as demonstrated by objcopy.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:24Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
An issue was discovered in GNU patch through 2.7.6. There is a segmentation fault, associated with a NULL pointer dereference, leading to a denial of service in the intuit_diff_type function in pch.c, aka a "mangled rename" issue.	Medium	security	JFrog	debian:stretch:patch	All Versions		2019-11-14T07:56:24Z
In the GetOpenCLCachedFilesDirectory function in magick/opencl.c in ImageMagick 7.0.7, a NULL pointer dereference vulnerability occurs because a memory allocation result is not checked, related to GetOpenCLCacheDirectory.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:24Z
MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos database to cause a denial of service (NULL pointer dereference) or bypass a DN container check by supplying tagged data that is internal to the database module.	Medium	security	JFrog	debian:stretch:krb5	All Versions		2019-11-14T07:56:24Z
The cr_tknzr_parse_comment function in cr-tknzr.c in libcroco 0.6.12 allows remote attackers to cause a denial of service (memory allocation error) via a crafted CSS file.	Medium	security	JFrog	debian:stretch:libcroco	All Versions		2019-11-14T07:55:57Z
ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadMATImage in coders\mat.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:07Z
An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.29 and 2.30. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_nested_args, demangle_args, do_arg, and do_type.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:24Z
GnuPG 2.2.4 and 2.2.5 does not enforce a configuration in which key certification requires an offline master Certify key, which results in apparently valid certifications that occurred only with access to a signing subkey.	Medium	security	JFrog	debian:stretch:gnupg2	All Versions		2019-11-14T07:56:25Z
In ImageMagick 7.0.6-3, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:07Z
The xz_head function in xzlib.c in libxml2 before 2.9.6 allows remote attackers to cause a denial of service (memory consumption) via a crafted LZMA file, because the decoder functionality does not restrict memory usage to what is required for a legitimate file.	Medium	security	JFrog	debian:stretch:libxml2	All Versions		2019-11-14T07:56:25Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
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.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:27Z
In numbers.c in libxslt 1.1.33, an xsl:number with certain format strings could lead to a uninitialized read in xsltNumberFormatInsertNumbers. This could allow an attacker to discern whether a byte on the stack contains the characters A, a, I, i, or 0, or any other character.	Medium	security	JFrog	debian:stretch:libxslt	All Versions		2019-11-14T07:52:56Z
MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos database to circumvent a DN containership check by supplying both a "linkdn" and "containerdn" database argument, or by supplying a DN string which is a left extension of a container DN string but is not hierarchically within the container DN.	Medium	security	JFrog	debian:stretch:krb5	All Versions		2019-11-14T07:56:22Z
Floating Point Exception (aka FPE or divide by zero) in opj_pi_next_cprl function in openjp2/pi.c:523 in OpenJPEG 2.1.2.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:54:26Z
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.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:55:20Z
The print_insn_score32 function in opcodes/score7-dis.c:552 in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
kernel drivers before version 4.17-rc1 are vulnerable to a weakness in the Linux kernel's implementation of random seed data. Programs, early in the boot sequence, could use the data allocated for the seed before it was sufficiently generated.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:56:27Z
ImageMagick version 7.0.7-28 contains a memory leak in ReadYCBCRImage in coders/ycbcr.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:27Z
The xfs_dinode_verify function in fs/xfs/libxfs/xfs_inode_buf.c in the Linux kernel through 4.16.3 allows local users to cause a denial of service (xfs_ilock_attr_map_shared invalid pointer dereference) via a crafted xfs image.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:56:27Z
In ImageMagick 7.0.7-28, there is an infinite loop in the ReadOneMNGImage function of the coders/png.c file. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted mng file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:28Z
NULL pointer dereference vulnerability in the rebuild_vlists function in lib/dotgen/conc.c in the dotgen library in Graphviz 2.40.1 allows remote attackers to cause a denial of service (application crash) via a crafted file.	Medium	security	JFrog	debian:stretch:graphviz	All Versions		2019-11-14T07:56:28Z
LibTIFF 4.0.9 has a NULL pointer dereference in the jpeg_fdct_16x16 function in jfdctint.c.	Medium	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:56:28Z
opcodes/i386-dis.c in GNU Binutils 2.28 does not consider the number of registers for bnd mode, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z
ImageMagick 7.0.6-2 has a memory leak vulnerability in WriteMAPImage in coders/map.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:07Z
The ignore_section_sym function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, does not validate the output_section pointer in the case of a symtab entry with a "SECTION" type that has a "0" value, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file, as demonstrated by objcopy.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:28Z
ImageMagick version 7.0.7-28 contains a memory leak in WriteTIFFImage in coders/tiff.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:29Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The aarch64_ext_ldst_reglist function in opcodes/aarch64-dis.c in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z
procps-ng, procps is vulnerable to a process hiding through race condition. Since the kernel's proc_pid_readdir() returns PID entries in ascending numeric order, a process occupying a high PID can use inotify events to determine when the process list is being scanned, and fork/exec to obtain a lower PID, thus avoiding enumeration. An unprivileged attacker can hide a process from procps-ng's utilities by exploiting a race condition in reading /proc/PID entries. This vulnerability affects procps and procps-ng up to version 3.3.15, newer versions might be affected also.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:56:29Z
In ImageMagick 7.0.7-20 Q16 x86_64, a memory leak vulnerability was found in the function GetImagePixelCache in MagickCore/cache.c, which allows attackers to cause a denial of service via a crafted CALS image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:30Z
Directory traversal vulnerability in util.c in GNU patch 2.6.1 and earlier allows user-assisted remote attackers to create or overwrite arbitrary files via a filename that is specified with a .. (dot dot) or full pathname, a related issue to CVE-2010-1679.	Medium	security	JFrog	debian:stretch:patch	All Versions		2019-11-14T07:54:26Z
opcodes/rl78-decode.opc in GNU Binutils 2.28 has an unbounded GETBYTE macro, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z
An exploitable integer overflow vulnerability exists in the tiff_image_parse functionality of Gdk-Pixbuf 2.36.6 when compiled with Clang. A specially crafted tiff file can cause a heap-overflow resulting in remote code execution. An attacker can send a file or a URL to trigger this vulnerability.	Medium	security	JFrog	debian:stretch:gdk-pixbuf	All Versions		2019-11-14T07:56:07Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
An issue was discovered in arm_pt 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_arm_hp_template, demangle_class_name, demangle_fund_type, do_type, do_arg, demangle_args, and demangle_nested_args. This can occur during execution of nm-new.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:30Z
libjpeg-turbo 1.5.90 is vulnerable to a denial of service vulnerability caused by a divide by zero when processing a crafted BMP image.	Medium	security	JFrog	debian:stretch:libjpeg-turbo	All Versions		2019-11-14T07:52:31Z
In the Linux kernel 4.15.0, a NULL pointer dereference was discovered in hfs_ext_read_extent in hfs.ko. This can occur during a mount of a crafted hfs filesystem.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:31Z
demangle_template in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30, allows attackers to trigger excessive memory consumption (aka OOM) during the "Create an array for saving the template argument values" XNEWVEC call. This can occur during execution of objdump.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:32Z
decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
The ReadMAGICKImage function in coders/magick.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:03Z
In PolicyKit (aka polkit) 0.115, the "start time" protection mechanism can be bypassed because fork() is not atomic, and therefore authorization decisions are improperly cached. This is related to lack of uid checking in polkitbackend/polkitbackendinteractiveauthority.c.	Medium	security	JFrog	debian:stretch:linux	< 4.9.161-1	>= 4.9.161-1	2019-11-14T07:52:45Z
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.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:53:56Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
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.	Medium	security	JFrog	debian:stretch:cairo	All Versions		2019-11-14T07:52:45Z
read_formatted_entries in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, does not properly validate the format count, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file, related to concat_filename.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, does not validate the DW_AT_name data type, which allows remote attackers to cause a denial of service (bfd_hash_hash NULL pointer dereference, or out-of-bounds access, and application crash) via a crafted ELF file, related to scan_unit_for_symbols and parse_comp_unit.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
A NULL pointer dereference (aka SEGV on unknown address 0x000000000000) was discovered in work_stuff_copy_to_from in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. This can occur during execution of objdump.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:32Z
An issue was discovered in elfutils 0.175. A segmentation fault can occur in the function elf64_xlatetom in libelf/elf32_xlatetom.c, due to dwfl_segment_report_module not checking whether the dyn data read from a core file is truncated. A crafted input can cause a program crash, leading to denial-of-service, as demonstrated by eu-stack.	Medium	security	JFrog	debian:stretch:elfutils	All Versions		2019-11-14T07:52:46Z
ImageMagick 7.0.7-2 has a memory leak in ReadOneJNGImage in coders/png.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:11Z
A heap-based buffer over-read was discovered in the function read_srclines in dwarf_getsrclines.c in libdw in elfutils 0.175. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by eu-nm.	Medium	security	JFrog	debian:stretch:elfutils	All Versions		2019-11-14T07:52:47Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The ethtool_get_wol function in net/core/ethtool.c in the Linux kernel through 4.7, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not initialize a certain data structure, which allows local users to obtain sensitive information via a crafted application, aka Android internal bug 28803952 and Qualcomm internal bug CR570754.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:55:48Z
In ImageMagick before 7.0.8-25 and GraphicsMagick through 1.3.31, several memory leaks exist in WritePDFImage in coders/pdf.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:47Z
Git through 2.14.2 mishandles layers of tree objects, which allows remote attackers to cause a denial of service (memory consumption) via a crafted repository, aka a Git bomb. This can also have an impact of disk consumption; however, an affected process typically would not survive its attempt to build the data structure in memory before writing to disk.	Medium	security	JFrog	debian:stretch:git	All Versions		2019-11-14T07:56:11Z
In the Linux kernel before 4.20.8, kvm_ioctl_create_device in virt/kvm/kvm_main.c mishandles reference counting because of a race condition, leading to a use-after-free.	Medium	security	JFrog	debian:stretch:linux	< 4.9.161-1	>= 4.9.161-1	2019-11-14T07:52:47Z
Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363.	Medium	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u3	>= 4.9.168-1+deb9u3	2019-11-14T07:52:56Z
In elfutils 0.175, a heap-based buffer over-read was discovered in the function elf32_xlatetom in elf32_xlatetom.c in libelf. A crafted ELF input can cause a segmentation fault leading to denial of service (program crash) because ebl_core_note does not reject malformed core file notes.	Medium	security	JFrog	debian:stretch:elfutils	All Versions		2019-11-14T07:52:47Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, miscalculates DW_FORM_ref_addr die refs in the case of a relocatable object file, which allows remote attackers to cause a denial of service (find_abstract_instance_name invalid memory read, segmentation fault, and application crash).	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:13Z
do_core_note in readelf.c in libmagic.a in file 5.35 has a stack-based buffer over-read, related to file_printable, a different vulnerability than CVE-2018-10360.	Medium	security	JFrog	debian:stretch:file	All Versions		2019-11-14T07:52:49Z
The bfd_mach_o_read_symtab_strtab function in bfd/mach-o.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap write and possibly achieve code execution via a crafted mach-o file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:04Z
An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.32. It is a heap-based buffer over-read in d_expression_1 in cp-demangle.c after many recursive calls.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:49Z
An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.32. It is a stack consumption issue in d_count_templates_scopes in cp-demangle.c after many recursive calls.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:49Z
An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an attempted excessive memory allocation in _bfd_elf_slurp_version_tables in elf.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:49Z
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.	Medium	security	JFrog	debian:stretch:openldap	All Versions		2019-11-14T07:54:42Z
An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an attempted excessive memory allocation in setup_group in elf.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:49Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The _bfd_elf_parse_gnu_properties function in elf-properties.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not prevent negative pointers, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) or possibly have unspecified other impact via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:15Z
Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.	Medium	security	JFrog	debian:stretch:python2.7	All Versions		2019-11-14T07:52:50Z
The alpha_vms_object_p function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap write and possibly achieve code execution via a crafted vms alpha file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:04Z
get_8bit_row in rdbmp.c in libjpeg-turbo through 1.5.90 and MozJPEG through 3.3.1 allows attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted 8-bit BMP in which one or more of the color indices is out of range for the number of palette entries.	Medium	security	JFrog	debian:stretch:libjpeg-turbo	All Versions		2019-11-14T07:52:50Z
parser.c in libxml2 before 2.9.5 does not prevent infinite recursion in parameter entities.	Medium	security	JFrog	debian:stretch:libxml2	All Versions		2019-11-14T07:56:15Z
An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH packets with a padding length value greater than the packet length are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	Medium	security	JFrog	debian:stretch:libssh2	< 1.7.0-1+deb9u1	>= 1.7.0-1+deb9u1	2019-11-14T07:52:50Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. There is a heap-based buffer over-read in _bfd_doprnt in bfd.c because elf_object_p in elfcode.h mishandles an e_shstrndx section of type SHT_GROUP by omitting a trailing '\0' character.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:56Z
An out of bounds read flaw was discovered in libssh2 before 1.8.1 when a specially crafted SFTP packet is received from the server. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	Medium	security	JFrog	debian:stretch:libssh2	< 1.7.0-1+deb9u1	>= 1.7.0-1+deb9u1	2019-11-14T07:52:50Z
The _bfd_vms_save_sized_string function in vms-misc.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:04Z
An issue was discovered in lib\cdt\dttree.c in libcdt.a in graphviz 2.40.1. Stack consumption occurs because of recursive agclose calls in lib\cgraph\graph.c in libcgraph.a, related to agfstsubg in lib\cgraph\subg.c.	Medium	security	JFrog	debian:stretch:graphviz	All Versions		2019-11-14T07:52:50Z
pax_decode_header in sparse.c in GNU Tar before 1.32 had a NULL pointer dereference when parsing certain archives that have malformed extended headers.	Medium	security	JFrog	debian:stretch:tar	All Versions		2019-11-14T07:52:50Z
urllib in Python 2.x through 2.7.16 supports the local_file: scheme, which makes it easier for remote attackers to bypass protection mechanisms that blacklist file: URIs, as demonstrated by triggering a urllib.urlopen('local_file:///etc/passwd') call.	Medium	security	JFrog	debian:stretch:python2.7	All Versions		2019-11-14T07:52:51Z
A vulnerability was found in gnutls versions from 3.5.8 before 3.6.7. A memory corruption (double free) vulnerability in the certificate verification API. Any client or server application that verifies X.509 certificates with GnuTLS 3.5.8 or later is affected.	Medium	security	JFrog	debian:stretch:gnutls28	All Versions		2019-11-14T07:52:51Z
In ImageMagick 7.0.8-36 Q16, there is a heap-based buffer over-read in the function WriteTIFFImage of coders/tiff.c, which allows an attacker to cause a denial of service or information disclosure via a crafted image file.	Medium	security	JFrog	debian:stretch:imagemagick	< 8:6.9.7.4+dfsg-11+deb9u7	>= 8:6.9.7.4+dfsg-11+deb9u7	2019-11-14T07:52:51Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
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.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:55:51Z
SQLite 3.25.2, when queries are run on a table with a malformed PRIMARY KEY, allows remote attackers to cause a denial of service (application crash) by leveraging the ability to run arbitrary SQL statements (such as in certain WebSQL use cases).	Medium	security	JFrog	debian:stretch:sqlite3	All Versions		2019-11-14T07:52:51Z
The bfd_cache_close function in bfd/cache.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause a heap use after free and possibly achieve code execution via a crafted nested archive file. This issue occurs because incorrect functions are called during an attempt to release memory. The issue can be addressed by better input validation in the bfd_generic_archive_p function in bfd/archive.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:04Z
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.	Medium	security	JFrog	debian:stretch:libxslt	All Versions		2019-11-14T07:55:51Z
libxml2 2.9.4 and earlier, as used in XMLSec 1.2.23 and earlier and other products, does not offer a flag directly indicating that the current document may be read but other files may not be opened, which makes it easier for remote attackers to conduct XML External Entity (XXE) attacks via a crafted document.	Medium	security	JFrog	debian:stretch:libxml2	All Versions		2019-11-14T07:54:01Z
In ncurses 6.1, there is a NULL pointer dereference at function _nc_parse_entry in parse_entry.c that will lead to a denial of service attack. The product proceeds to the dereference code path even after a "dubious character `*' in name or alias field" detection.	Medium	security	JFrog	debian:stretch:ncurses	All Versions		2019-11-14T07:52:52Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The bfd_mach_o_i386_canonicalize_one_reloc function in bfd/mach-o-i386.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted mach-o file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:04Z
In ImageMagick 7.0.7-16 Q16, a memory leak vulnerability was found in the function WriteOnePNGImage in coders/png.c, which allows attackers to cause a denial of service via a crafted PNG image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z
ImageMagick 7.0.8-34 has a memory leak in the ReadPCLImage function in coders/pcl.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:56Z
ReadXWDImage in coders/xwd.c in the XWD image parsing component of ImageMagick 7.0.8-41 Q16 allows attackers to cause a denial-of-service (divide-by-zero error) by crafting an XWD image file in which the header indicates neither LSB first nor MSB first.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:52Z
The nlm_swap_auxiliary_headers_in function in bfd/nlmcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted nlm file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:04Z
An infinite loop issue was found in the vhost_net kernel module in Linux Kernel up to and including v5.1-rc6, while handling incoming packets in handle_rx(). It could occur if one end sends packets faster than the other end can process them. A guest user, maybe remote one, could use this flaw to stall the vhost_net kernel thread, resulting in a DoS scenario.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:53Z
In ImageMagick 7.0.6-2, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
In ImageMagick 7.0.8-40 Q16, there is a heap-based buffer over-read in the function WritePNMImage of coders/pnm.c, which allows an attacker to cause a denial of service or possibly information disclosure via a crafted image file. This is related to SetGrayscaleImage in MagickCore/quantize.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:53Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In ImageMagick 7.0.6-2, a memory leak vulnerability was found in the function ReadMVGImage in coders/mvg.c, which allows attackers to cause a denial of service, related to the function ReadSVGImage in svg.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	Medium	security	JFrog	debian:stretch:mariadb-10.1	All Versions		2019-11-14T07:52:53Z
ImageMagick 7.0.6-2 has a memory leak vulnerability in WriteINLINEImage in coders/inline.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:05Z
In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadPSDChannelZip in coders/psd.c, which allows attackers to cause a denial of service via a crafted psd image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z
In ImageMagick 7.0.7-17 Q16, there are memory leaks in ReadRLAImage in coders/rla.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z
In ImageMagick 7.0.7-12 Q16, there are memory leaks in MontageImageCommand in MagickWand/montage.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z
ImageMagick before 7.0.8-50 has a "use of uninitialized value" vulnerability in the function ReadCUTImage in coders/cut.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:56Z
Microarchitectural Store Buffer Data Sampling (MSBDS): Store buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf	Medium	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u2	>= 4.9.168-1+deb9u2	2019-11-14T07:52:53Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
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.	Medium	security	JFrog	debian:stretch:openldap	All Versions		2019-11-14T07:56:17Z
** DISPUTED ** 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.	Medium	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:56:17Z
The elf_object_p function in elfcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, has an unsigned integer overflow because bfd_size_type multiplication is not used. A crafted ELF file allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:20Z
stack_protect_prologue in cfgexpand.c and stack_protect_epilogue in function.c in GNU Compiler Collection (GCC) 4.1 through 8 (under certain circumstances) generate instruction sequences when targeting ARM targets that spill the address of the stack protector guard, which allows an attacker to bypass the protection of -fstack-protector, -fstack-protector-all, -fstack-protector-strong, and -fstack-protector-explicit against stack overflow by controlling what the stack canary is compared against.	Medium	security	JFrog	debian:stretch:gcc-6	All Versions		2019-11-14T07:52:55Z
ImageMagick 7.0.7-22 Q16 has memory leaks in the EncodeImageAttributes function in coders/json.c, as demonstrated by the ReadPSDLayersInternal function in coders/psd.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:18Z
In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allow remote attackers to cause a denial of service via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:18Z
The print_symbol_for_build_attribute function in readelf.c in GNU Binutils 2017-04-12 allows remote attackers to cause a denial of service (invalid read and SEGV) via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:55Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In ImageMagick 7.0.6-10 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allow remote attackers to cause a denial of service via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:18Z
An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. The pre-defined function "strlen" is getting a "NULL" string as a parameter value in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the Key Distribution Center (KDC), which allows remote authenticated users to cause a denial of service (NULL pointer dereference) via a modified kadmin client.	Medium	security	JFrog	debian:stretch:krb5	All Versions		2019-11-14T07:56:18Z
In systemd prior to 234 a race condition exists between .mount and .automount units such that automount requests from kernel may not be serviced by systemd resulting in kernel holding the mountpoint and any processes that try to use said mount will hang. A race condition like this may lead to denial of service, until mount points are unmounted.	Medium	security	JFrog	debian:stretch:systemd	< 232-25+deb9u10	>= 232-25+deb9u10	2019-11-14T07:56:18Z
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.	Medium	security	JFrog	debian:stretch:libwmf	All Versions		2019-11-14T07:55:03Z
An issue was discovered in the Linux kernel before 4.20.15. The nfc_llcp_build_tlv function in net/nfc/llcp_commands.c may return NULL. If the caller does not check for this, it will trigger a NULL pointer dereference. This will cause denial of service. This affects nfc_llcp_build_gb in net/nfc/llcp_core.c.	Medium	security	JFrog	debian:stretch:linux	< 4.9.168-1	>= 4.9.168-1	2019-11-14T07:52:56Z
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.	Medium	security	JFrog	debian:stretch:krb5	All Versions		2019-11-14T07:56:20Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In Libgcrypt 1.8.4, the C implementation of AES is vulnerable to a flush-and-reload side-channel attack because physical addresses are available to other processes. (The C implementation is used on platforms where an assembly-language implementation is unavailable.)	Medium	security	JFrog	debian:stretch:libgcrypt20	All Versions		2019-11-14T07:52:56Z
The NIST SP 800-90A default statement of the Dual Elliptic Curve Deterministic Random Bit Generation (Dual_EC_DRBG) algorithm contains point Q constants with a possible relationship to certain "skeleton key" values, which might allow context-dependent attackers to defeat cryptographic protection mechanisms by leveraging knowledge of those values. NOTE: this is a preliminary CVE for Dual_EC_DRBG; future research may provide additional details about point Q and associated attacks, and could potentially lead to a RECAST or REJECT of this CVE.	Medium	security	JFrog	debian:stretch:openssl	All Versions		2019-11-14T07:55:06Z
A NULL pointer dereference vulnerability in the function nfc_genl_deactivate_target() in net/nfc/netlink.c in the Linux kernel before 5.1.13 can be triggered by a malicious user-mode program that omits certain NFC attributes, leading to denial of service.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:56Z
In the ReadDCMImage function in coders/dcm.c in ImageMagick before 7.0.7-23, each redmap, greenmap, and bluemap variable can be overwritten by a new pointer. The previous pointer is lost, which leads to a memory leak. This allows remote attackers to cause a denial of service.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:20Z
ImageMagick 7.0.8-34 has a "use of uninitialized value" vulnerability in the WriteJP2Image function in coders/jp2.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:56Z
Linux kernel 2.4 and 2.6 allows attackers to cause a denial of service (memory exhaustion and panic) by creating a large number of connected file descriptors or socketpairs and setting a large data transfer buffer, then preventing Linux from being able to finish the transfer by causing the process to become a zombie, or closing the file descriptor without closing an associated reference.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:54:11Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In OpenJPEG 2.3.1, there is excessive iteration in the opj_t1_encode_cblks function of openjp2/t1.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file. This issue is similar to CVE-2018-6616.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:52:56Z
In GNU Binutils 2.30, there's an integer overflow in the function load_specific_debug_section() in objdump.c, which results in `malloc()` with 0 size. A crafted ELF file allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:21Z
ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadPSImage in coders/ps.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:56Z
The acpi_ds_create_operands() function in drivers/acpi/acpica/dsutils.c in the Linux kernel through 4.12.9 does not flush the operand cache and causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism (in the kernel through 4.9) via a crafted ACPI table.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:56:05Z
In uvc_parse_standard_control of uvc_driver.c, there is a possible out-of-bound read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-111760968.	Medium	security	JFrog	debian:stretch:linux	< 4.9.168-1	>= 4.9.168-1	2019-11-14T07:52:57Z
The bfd_section_from_shdr function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (segmentation fault) via a large attribute section.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:22Z
ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of a wand/mogrify.c error.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
In OpenEXR 2.2.0, an invalid write of size 1 in the bufferedReadPixels function in ImfInputFile.cpp could cause the application to crash or execute arbitrary code.	Medium	security	JFrog	debian:stretch:openexr	All Versions		2019-11-14T07:55:56Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The Linux kernel 4.x (starting from 4.1) and 5.x before 5.0.8 allows Information Exposure (partial kernel address disclosure), leading to a KASLR bypass. Specifically, it is possible to extract the KASLR kernel image offset using the IP ID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). This key contains enough bits from a kernel address (of a static variable) so when the key is extracted (via enumeration), the offset of the kernel image is exposed. This attack can be carried out remotely, by the attacker forcing the target device to send UDP or ICMP (or certain other) traffic to attacker-controlled IP addresses. Forcing a server to send UDP traffic is trivial if the server is a DNS server. ICMP traffic is trivial if the server answers ICMP Echo requests (ping). For client targets, if the target visits the attacker's web page, then WebRTC or gQUIC can be used to force UDP traffic to attacker-controlled IP addresses. NOTE: this attack against KASLR became viable in 4.1 because IP ID generation was changed to have a dependency on an address associated with a network namespace.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:57Z
The ReadTIFFImage function in coders/tiff.c in ImageMagick 7.0.7-23 Q16 does not properly validate the amount of image data in a file, which allows remote attackers to cause a denial of service (memory allocation failure in the AcquireMagickMemory function in MagickCore/memory.c).	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:22Z
ImageMagick 7.0.8-50 Q16 has memory leaks in AcquireMagickMemory because of an AnnotateImage error.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
The setup_group function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a group section that is too small.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:05Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In ImageMagick 7.0.8-50 Q16, ComplexImages in MagickCore/fourier.c has a heap-based buffer over-read because of incorrect calls to GetCacheViewVirtualPixels.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
An issue was discovered in GNU patch before 2.7.6. Out-of-bounds access within pch_write_line() in pch.c can possibly lead to DoS via a crafted input file.	Medium	security	JFrog	debian:stretch:patch	All Versions		2019-11-14T07:56:22Z
The parse_die function in dwarf1.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (integer overflow and application crash) via an ELF file with corrupt dwarf1 debug information, as demonstrated by nm.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:22Z
The score_opcodes function in opcodes/score7-dis.c in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z
ImageMagick 7.0.6-2 has a memory leak vulnerability in WritePDFImage in coders/pdf.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:07Z
ntfs_read_locked_inode in the ntfs.ko filesystem driver in the Linux kernel 4.15.0 allows attackers to trigger a use-after-free read and possibly cause a denial of service (kernel oops or panic) via a crafted ntfs filesystem.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:32Z
In libssh2 before 1.9.0, kex_method_diffie_hellman_group_exchange_sha256_key_exchange in kex.c has an integer overflow that could lead to an out-of-bounds read in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server. This is related to an _libssh2_check_length mistake, and is different from the various issues fixed in 1.8.1, such as CVE-2019-3855.	Medium	security	JFrog	debian:stretch:libssh2	All Versions		2019-11-14T07:52:57Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In ImageMagick 7.0.6-6, a memory leak vulnerability was found in the function WriteOneJNGImage in coders/png.c, which allows attackers to cause a denial of service (WriteJNGImage memory consumption) via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:05Z
In the Linux kernel through 5.2.1 on the powerpc platform, when hardware transactional memory is disabled, a local user can cause a denial of service (TM Bad Thing exception and system crash) via a sigreturn() system call that sends a crafted signal frame. This affects arch/powerpc/kernel/signal_32.c and arch/powerpc/kernel/signal_64.c.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:58Z
In OpenEXR 2.2.0, an invalid write of size 8 in the storeSSE function in ImfOptimizedPixelReading.h could cause the application to crash or execute arbitrary code.	Medium	security	JFrog	debian:stretch:openexr	All Versions		2019-11-14T07:55:56Z
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.	Medium	security	JFrog	debian:stretch:libgcrypt20	All Versions		2019-11-14T07:56:23Z
The display_debug_ranges function in dwarf.c in GNU Binutils 2.30 allows remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, as demonstrated by objdump.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:22Z
A heap-based buffer overflow exists in Info-Zip UnZip version <= 6.00 in the processing of password-protected archives that allows an attacker to perform a denial of service or to possibly achieve code execution.	Medium	security	JFrog	debian:stretch:unzip	< 6.0-21+deb9u1	>= 6.0-21+deb9u1	2019-11-14T07:56:23Z
An issue was discovered in ImageMagick 7.0.7-22 Q16. The IsWEBPImageLossless function in coders/webp.c allows attackers to cause a denial of service (segmentation violation) via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:23Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
Stack consumption vulnerability in the regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (resource exhaustion) via a regular expression containing adjacent repetition operators, as demonstrated by a {10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for ProFTPD.	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:55:19Z
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: XML). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	Medium	security	JFrog	debian:stretch:mariadb-10.1	All Versions		2019-11-14T07:52:58Z
The assign_file_positions_for_non_load_sections function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an ELF file with a RELRO segment that lacks a matching LOAD segment, as demonstrated by objcopy.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:23Z
In OpenEXR 2.2.0, an invalid read of size 1 in the uncompress function in ImfZip.cpp could cause the application to crash.	Medium	security	JFrog	debian:stretch:openexr	All Versions		2019-11-14T07:55:56Z
ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of a misplaced strncpy and an off-by-one error.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
Heap-based buffer overflow in the cpSeparateBufToContigBuf function in tiffcp.c in LibTIFF 4.0.9 allows remote attackers to cause a denial of service (crash) or possibly have unspecified other impact via a crafted TIFF file.	Medium	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:52:32Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (integer underflow or overflow, and application crash) via an ELF file with a corrupt DWARF FORM block, as demonstrated by nm.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:24Z
ImageMagick 7.0.6-2 has a memory leak vulnerability in WritePCXImage in coders/pcx.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:06Z
In OpenEXR 2.2.0, an invalid read of size 1 in the refill function in ImfFastHuf.cpp could cause the application to crash.	Medium	security	JFrog	debian:stretch:openexr	All Versions		2019-11-14T07:55:56Z
In ImageMagick before 6.9.9-3 and 7.x before 7.0.6-3, there is a missing NULL check in the ReadMATImage function in coders/mat.c, leading to a denial of service (assertion failure and application exit) in the DestroyImageInfo function in MagickCore/image.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:08Z
A Stack Exhaustion issue was discovered in debug_write_type in debug.c in GNU Binutils 2.30 because of DEBUG_KIND_INDIRECT infinite recursion.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:32Z
The bfd_get_debug_link_info_1 function in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, has an unchecked strnlen operation. Remote attackers could leverage this vulnerability to cause a denial of service (segmentation fault) via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:24Z
ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadOneJNGImage in coders\png.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:06Z
An issue was discovered in ImageMagick 7.0.7. A memory leak vulnerability was found in the function ReadPCDImage in coders/pcd.c, which allow remote attackers to cause a denial of service via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:24Z
The XFS subsystem in the Linux kernel through 4.8.2 allows local users to cause a denial of service (fdatasync failure and system hang) by using the vfs syscall group in the trinity program, related to a "page lock order bug in the XFS seek hole/data implementation."	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:55:19Z
In ImageMagick 7.0.7-24 Q16, there is a heap-based buffer over-read in IsWEBPImageLossless in coders/webp.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:24Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, does not validate the PLT section size, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to elf_i386_get_synthetic_symtab in elf32-i386.c and elf_x86_64_get_synthetic_symtab in elf64-x86-64.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:07Z
ImageMagick 7.0.7-26 Q16 has excessive iteration in the DecodeLabImage and EncodeLabImage functions (coders/tiff.c), which results in a hang (tens of minutes) with a tiny PoC file. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted tiff file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:25Z
nghttp2 version >= 1.10.0 and nghttp2 <= v1.31.0 contains an Improper Input Validation CWE-20 vulnerability in ALTSVC frame handling that can result in segmentation fault leading to denial of service. This attack appears to be exploitable via network client. This vulnerability appears to have been fixed in >= 1.31.1.	Medium	security	JFrog	debian:stretch:nghttp2	All Versions		2019-11-14T07:56:26Z
In ImageMagick 7.0.6-3, missing validation was found in coders/mat.c, leading to an assertion failure in the function DestroyImage in MagickCore/image.c, which allows attackers to cause a denial of service.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:07Z
An issue was discovered in fs/xfs/xfs_icache.c in the Linux kernel through 4.17.3. There is a NULL pointer dereference and panic in lookup_slow() on a NULL inode->i_ops pointer when doing pathwalks on a corrupted xfs image. This occurs because of a lack of proper validation that cached inodes are free during allocation.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:32Z
In the Linux kernel before 5.1.7, a device can be tracked by an attacker using the IP ID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). An attack may be conducted by hosting a crafted web page that uses WebRTC or gQUIC to force UDP traffic to attacker-controlled IP addresses.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:57Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
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.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:54:26Z
The process_otr function in bfd/versados.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, does not validate a certain offset, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z
The dump_callback function in SQLite 3.20.0 allows remote attackers to cause a denial of service (EXC_BAD_ACCESS and application crash) via a crafted file.	Medium	security	JFrog	debian:stretch:sqlite3	All Versions		2019-11-14T07:56:08Z
The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted ELF file, as demonstrated by _bfd_elf_parse_attributes in elf-attrs.c and bfd_malloc in libbfd.c. This can occur during execution of nm.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:32Z
process_cu_tu_index in dwarf.c in GNU Binutils 2.30 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted binary file, as demonstrated by readelf.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:27Z
In ImageMagick 7.0.6-6, a memory leak vulnerability was found in the function WritePCXImage in coders/pcx.c, which allows attackers to cause a denial of service via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:07Z
The _bfd_vms_slurp_etir function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In ncurses before 6.1.20180414, there is a NULL Pointer Dereference in the _nc_parse_entry function of tinfo/parse_entry.c. It could lead to a remote denial of service if the terminfo library code is used to process untrusted terminfo data in which a use-name is invalid syntax. The product proceeds to the dereference code path even after a "dubious character `[' in name or alias field" detection.	Medium	security	JFrog	debian:stretch:ncurses	All Versions		2019-11-14T07:56:28Z
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.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:56:07Z
concat_filename in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted binary file, as demonstrated by nm-new.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:28Z
The _bfd_XX_bfd_copy_private_bfd_data_common function in peXXigen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, processes a negative Data Directory size with an unbounded loop that increases the value of (external_IMAGE_DEBUG_DIRECTORY) *edd so that the address exceeds its own memory region, resulting in an out-of-bounds memory write, as demonstrated by objcopy copying private info with _bfd_pex64_bfd_copy_private_bfd_data_common in pex64igen.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:29Z
In ImageMagick 7.0.6-5, a length-validation vulnerability was found in the function ReadPSDLayersInternal in coders/psd.c, which allows attackers to cause a denial of service (ReadPSDImage memory exhaustion) via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:07Z
In ImageMagick 7.0.8-4, there is a memory leak in the XMagickCommand function in MagickCore/animate.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:32Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
A vulnerability was found in libexif. An integer overflow when parsing the MNOTE entry data of the input file. This can cause Denial-of-Service (DoS) and Information Disclosure (disclosing some critical heap chunk metadata, even other applications' private data).	Medium	security	JFrog	debian:stretch:libexif	All Versions		2019-11-14T07:56:07Z
In ImageMagick 7.0.7-20 Q16 x86_64, a memory leak vulnerability was found in the function ReadDCMImage in coders/dcm.c, which allows attackers to cause a denial of service via a crafted DCM image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:30Z
In the coff_pointerize_aux function in coffgen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, an index is not validated, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted file, as demonstrated by objcopy of a COFF object.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:22Z
** DISPUTED ** An issue was discovered in the Linux kernel through 4.17.2. Since the page allocator does not yield CPU resources to the owner of the oom_lock mutex, a local unprivileged user can trivially lock up the system forever by wasting CPU resources from the page allocator (e.g., via concurrent page fault events) when the global OOM killer is invoked. NOTE: the software maintainer has not accepted certain proposed patches, in part because of a viewpoint that "the underlying problem is non-trivial to handle."	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:30Z
The read_section function in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (parse_comp_unit heap-based buffer over-read and application crash) via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:08Z
The mpatch_apply function in mpatch.c in Mercurial before 4.6.1 incorrectly proceeds in cases where the fragment start is past the end of the original data, aka OVE-20180430-0004.	Medium	security	JFrog	debian:stretch:mercurial	All Versions		2019-11-14T07:52:32Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The ieee_object_p function in bfd/ieee.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, might allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. NOTE: this may be related to a compiler bug.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z
In ImageMagick before 6.9.8-5 and 7.x before 7.0.5-6, there is a memory leak in the ReadMATImage function in coders/mat.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:07Z
The _bfd_elf_parse_attributes function in elf-attrs.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (_bfd_elf_attr_strdup heap-based buffer over-read and application crash) via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:08Z
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.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:55:24Z
The ieee_archive_p function in bfd/ieee.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, might allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. NOTE: this may be related to a compiler bug.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z
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."	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:55:28Z
The decode_line_info function in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (read_1_byte heap-based buffer over-read and application crash) via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:08Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
remember_Ktype in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30, allows attackers to trigger excessive memory consumption (aka OOM). This can occur during execution of cxxfilt.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:32Z
The disassemble_bytes function in objdump.c in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of rae insns printing for this file during "objdump -D" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z
An issue was discovered in fs/xfs/libxfs/xfs_inode_buf.c in the Linux kernel through 4.17.3. A denial of service (memory corruption and BUG) can occur for a corrupted xfs image upon encountering an inode that is in extent format, but has more extents than fit in the inode fork.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:32Z
The getsym function in tekhex.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (stack-based buffer over-read and application crash) via a malformed tekhex binary.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:08Z
An issue was discovered in fs/xfs/libxfs/xfs_attr_leaf.c in the Linux kernel through 4.17.3. An OOPS may occur for a corrupted xfs image after xfs_da_shrink_inode() is called with a NULL bp.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:32Z
ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/threshold.c in AdaptiveThresholdImage because a width of zero is mishandled.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadMPCImage in coders\mpc.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:08Z
ImageMagick 7.0.8-4 has a memory leak for a colormap in WriteMPCImage in coders/mpc.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:33Z
The mpatch_decode function in mpatch.c in Mercurial before 4.6.1 mishandles certain situations where there should be at least 12 bytes remaining after the current position in the patch data, but actually are not, aka OVE-20180430-0001.	Medium	security	JFrog	debian:stretch:mercurial	All Versions		2019-11-14T07:52:32Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
opcodes/rx-decode.opc in GNU Binutils 2.28 lacks bounds checks for certain scale arrays, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z
Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a speculative buffer overflow and side-channel analysis.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:33Z
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.	Medium	security	JFrog	debian:stretch:libwmf	All Versions		2019-11-14T07:53:50Z
An issue was discovered in shadow 4.5. newgidmap (in shadow-utils) is setuid and allows an unprivileged user to be placed in a user namespace where setgroups(2) is permitted. This allows an attacker to remove themselves from a supplementary group, which may allow access to certain filesystem paths if the administrator has used "group blacklisting" (e.g., chmod g-rwx) to restrict access to paths. This flaw effectively reverts a security feature in the kernel (in particular, the /proc/self/setgroups knob) to prevent this sort of privilege escalation.	Medium	security	JFrog	debian:stretch:shadow	All Versions		2019-11-14T07:56:22Z
A NULL pointer dereference vulnerability exists in the xpath.c:xmlXPathCompOpEval() function of libxml2 through 2.9.8 when parsing an invalid XPath expression in the XPATH_OP_AND or XPATH_OP_OR case. Applications processing untrusted XSL format inputs with the use of the libxml2 library may be vulnerable to a denial of service attack due to a crash of the application.	Medium	security	JFrog	debian:stretch:libxml2	All Versions		2019-11-14T07:52:33Z
ImageMagick 7.0.8-4 has a memory leak in parse8BIM in coders/meta.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:33Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file in the _bfd_vms_get_value and _bfd_vms_slurp_etir functions during "objdump -D" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z
Memory leak in drivers/media/video/videobuf-core.c in the videobuf subsystem in the Linux kernel 2.6.x through 4.x allows local users to cause a denial of service (memory consumption) by leveraging /dev/video access for a series of mmap calls that require new allocations, a different vulnerability than CVE-2007-6761. NOTE: as of 2016-06-18, this affects only 11 drivers that have not been updated to use videobuf2 instead of videobuf.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:55:32Z
ImageMagick 7.0.8-4 has a memory leak in ReadMIFFImage in coders/miff.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:33Z
ImageMagick 7.0.8-4 has a memory leak in DecodeImage in coders/pcd.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:33Z
ReadWEBPImage in coders/webp.c in ImageMagick 7.0.6-5 has an issue where memory allocation is excessive because it depends only on a length field in a header.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:08Z
ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of an error in MagickWand/mogrify.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
The *regs* macros in opcodes/bfin-dis.c in GNU Binutils 2.28 allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z
ImageMagick 7.0.6-2 has a memory leak vulnerability in WriteMSLImage in coders/msl.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:08Z
An issue has been found in libpng 1.6.34. It is a SEGV in the function png_free_data in png.c, related to the recommended error handling for png_read_image.	Medium	security	JFrog	debian:stretch:libpng1.6	All Versions		2019-11-14T07:52:34Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The versados_mkobject function in bfd/versados.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, does not initialize a certain data structure, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z
An issue has been found in third-party PNM decoding associated with libpng 1.6.35. It is a stack-based buffer overflow in the function get_token in pnm2png.c in pnm2png.	Medium	security	JFrog	debian:stretch:libpng1.6	All Versions		2019-11-14T07:52:34Z
Division-by-zero vulnerabilities in the functions pi_next_pcrl, pi_next_cprl, and pi_next_rpcl in lib/openjp3d/pi.c in OpenJPEG through 2.3.0 allow remote attackers to cause a denial of service (application crash).	Medium	security	JFrog	debian:stretch:openjpeg2	< 2.1.2-1.1+deb9u3	>= 2.1.2-1.1+deb9u3	2019-11-14T07:52:34Z
libxml2 2.9.8, if --with-lzma is used, allows remote attackers to cause a denial of service (infinite loop) via a crafted XML file that triggers LZMA_MEMLIMIT_ERROR, as demonstrated by xmllint, a different vulnerability than CVE-2015-8035 and CVE-2018-9251.	Medium	security	JFrog	debian:stretch:libxml2	All Versions		2019-11-14T07:52:34Z
In task_get_unused_fd_flags of binder.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-69164715 References: Upstream kernel.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:34Z
In the function ReadTXTImage() in coders/txt.c in ImageMagick 7.0.6-10, an integer overflow might occur for the addition operation "GetQuantumRange(depth)+1" when "depth" is large, producing a smaller value than expected. As a result, an infinite loop would occur for a crafted TXT file that claims a very large "max_value" value.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:08Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
** DISPUTED ** 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.	Medium	security	JFrog	debian:stretch:glib2.0	All Versions		2019-11-14T07:53:27Z
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	Medium	security	JFrog	debian:stretch:mariadb-10.1	All Versions		2019-11-14T07:52:58Z
The sh_elf_set_mach_from_flags function in bfd/elf32-sh.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:57Z
The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, do not ensure a unique PLT entry for a symbol, which allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:09Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'	Medium	security	JFrog	debian:stretch:openssh	All Versions		2019-11-14T07:52:36Z
The get_build_id function in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file in which a certain size field is larger than a corresponding data field, as demonstrated by mishandling within the objdump program.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:58Z
In ImageMagick 7.0.7-1 Q16, the PersistPixelCache function in magick/cache.c mishandles the pixel cache nexus, which allows remote attackers to cause a denial of service (NULL pointer dereference in the function GetVirtualPixels in MagickCore/cache.c) via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
dwarf_getaranges in dwarf_getaranges.c in libdw in elfutils before 2018-08-18 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted file.	Medium	security	JFrog	debian:stretch:elfutils	All Versions		2019-11-14T07:52:36Z
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.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:56:05Z
In OpenEXR 2.2.0, an invalid read of size 1 in the getBits function in ImfHuf.cpp could cause the application to crash.	Medium	security	JFrog	debian:stretch:openexr	All Versions		2019-11-14T07:55:56Z
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.	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:52:57Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
A flaw was found in the Linux Kernel where an attacker may be able to have an uncontrolled read to kernel-memory from within a vm guest. A race condition between connect() and close() function may allow an attacker using the AF_VSOCK protocol to gather a 4 byte information leak or possibly intercept or corrupt AF_VSOCK messages destined to other clients.	Medium	security	JFrog	debian:stretch:linux	< 4.9.161-1	>= 4.9.161-1	2019-11-14T07:52:36Z
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.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:52:36Z
The getvalue function in tekhex.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (stack-based buffer over-read and application crash) via a crafted tekhex file, as demonstrated by mishandling within the nm program.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:58Z
libdw in elfutils 0.173 checks the end of the attributes list incorrectly in dwarf_getabbrev in dwarf_getabbrev.c and dwarf_hasattr in dwarf_hasattr.c, leading to a heap-based buffer over-read and an application crash.	Medium	security	JFrog	debian:stretch:elfutils	All Versions		2019-11-14T07:52:36Z
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.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:52:36Z
GNOME GLib 2.56.1 has an out-of-bounds read vulnerability in g_markup_parse_context_parse() in gmarkup.c, related to utf8_str().	Medium	security	JFrog	debian:stretch:glib2.0	All Versions		2019-11-14T07:52:37Z
ImageMagick 7.0.6-6 has a memory exhaustion vulnerability in ReadWPGImage in coders/wpg.c via a crafted wpg image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
The functions ReadDCMImage in coders/dcm.c, ReadPWPImage in coders/pwp.c, ReadCALSImage in coders/cals.c, and ReadPICTImage in coders/pict.c in ImageMagick 7.0.8-4 do not check the return value of the fputc function, which allows remote attackers to cause a denial of service via a crafted image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:37Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function ReadMPCImage in coders/mpc.c, which allows attackers to cause a denial of service via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
ImageMagick 7.0.8-5 has a memory leak vulnerability in the function ReadOneJNGImage in coders/png.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:37Z
OpenSSH 4.6 and earlier, when ChallengeResponseAuthentication is enabled, allows remote attackers to determine the existence of user accounts by attempting to authenticate via S/KEY, which displays a different response if the user account exists, a similar issue to CVE-2001-1483.	Medium	security	JFrog	debian:stretch:openssh	All Versions		2019-11-14T07:55:34Z
In ImageMagick 7.0.7-29 and earlier, a memory leak in the formatIPTCfromBuffer function in coders/meta.c was found.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:37Z
libexif through 0.6.21 is vulnerable to out-of-bounds heap read vulnerability in exif_data_save_data_entry function in libexif/exif-data.c caused by improper length computation of the allocated data of an ExifMnote entry which can cause denial-of-service or possibly information disclosure.	Medium	security	JFrog	debian:stretch:libexif	All Versions		2019-11-14T07:56:09Z
In ImageMagick 7.0.7-29 and earlier, a missing NULL check in ReadOneJNGImage in coders/png.c allows an attacker to cause a denial of service (WriteBlob assertion failure and application exit) via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:37Z
A NULL pointer dereference in the function _TIFFmemcmp at tif_unix.c (called from TIFFWriteDirectoryTagTransferfunction) in LibTIFF 4.0.9 allows an attacker to cause a denial-of-service through a crafted tiff file. This vulnerability can be triggered by the executable tiffcp.	Medium	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:52:37Z
The AcquireResampleFilterThreadSet function in magick/resample-private.h in ImageMagick 7.0.7-4 mishandles failed memory allocation, which allows remote attackers to cause a denial of service (NULL Pointer Dereference in DistortImage in MagickCore/distort.c, and application crash) via unspecified vectors.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
An issue was discovered in LibTIFF 4.0.9. There is a int32 overflow in multiply_ms in tools/ppm2tiff.c, which can cause a denial of service (crash) or possibly have unspecified other impact via a crafted image file.	Medium	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:52:38Z
An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31. An invalid memory access exists in bfd_zalloc in opncls.c. Attackers could leverage this vulnerability to cause a denial of service (application crash) via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:38Z
DrawGetStrokeDashArray in wand/drawing-wand.c in ImageMagick 7.0.7-1 mishandles certain NULL arrays, which allows attackers to perform Denial of Service (NULL pointer dereference and application crash in AcquireQuantumMemory within MagickCore/memory.c) by providing a crafted Image File as input.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31. a heap-based buffer over-read in bfd_getl32 in libbfd.c allows an attacker to cause a denial of service through a crafted PE file. This vulnerability can be triggered by the executable objdump.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:38Z
An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31. An invalid memory access exists in _bfd_stab_section_find_nearest_line in syms.c. Attackers could leverage this vulnerability to cause a denial of service (application crash) via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:38Z
ImageMagick 7.0.6-6 has a memory leak in ReadMATImage in coders/mat.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31. There is a NULL pointer dereference in work_stuff_copy_to_from when called from iterate_demangle_function.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:38Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In the Linux kernel through 4.15.4, the floppy driver reveals the addresses of kernel functions and global variables using printk calls within the function show_floppy in drivers/block/floppy.c. An attacker can read this information from dmesg and use the addresses to find the locations of kernel code and data and bypass kernel security protections such as KASLR.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:56:23Z
block/scsi_ioctl.c in the Linux kernel through 3.8 does not properly consider the SCSI device class during authorization of SCSI commands, which allows local users to bypass intended access restrictions via an SG_IO ioctl call that leverages overlapping opcodes.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:55:38Z
cairo-truetype-subset.c in cairo 1.15.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) because of mishandling of an unexpected malloc(0) call.	Medium	security	JFrog	debian:stretch:cairo	All Versions		2019-11-14T07:56:01Z
ImageMagick 7.0.7-28 has a memory leak vulnerability in WritePDBImage in coders/pdb.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:38Z
ImageMagick 7.0.7-28 has a memory leak vulnerability in WriteSGIImage in coders/sgi.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:38Z
ImageMagick 7.0.7-28 has a memory leak vulnerability in ReadBGRImage in coders/bgr.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:38Z
ImageMagick 7.0.6-8 Q16 mishandles EOF checks in ReadMPCImage in coders/mpc.c, leading to division by zero in GetPixelCacheTileSize in MagickCore/cache.c, allowing remote attackers to cause a denial of service via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
An issue was discovered in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31. There is a stack consumption problem caused by the cplus_demangle_type function making recursive calls to itself in certain scenarios involving many 'P' characters.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:38Z
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.	Medium	security	JFrog	debian:stretch:cairo	All Versions		2019-11-14T07:56:02Z
cext/manifest.c in Mercurial before 4.7.2 has an out-of-bounds read during parsing of a malformed manifest entry.	Medium	security	JFrog	debian:stretch:mercurial	All Versions		2019-11-14T07:52:38Z
ImageMagick 7.0.7-28 has a memory leak vulnerability in WritePCXImage in coders/pcx.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:38Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In ImageMagick 7.0.8-13 Q16, there is an infinite loop in the ReadBMPImage function of the coders/bmp.c file. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:38Z
In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:09Z
In ImageMagick 7.0.8-13 Q16, there is a heap-based buffer over-read in the EncodeImage function of coders/pict.c, which allows attackers to cause a denial of service via a crafted SVG image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:39Z
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.	Medium	security	JFrog	debian:stretch:gnutls28	All Versions		2019-11-14T07:55:39Z
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).	Medium	security	JFrog	debian:stretch:cairo	All Versions		2019-11-14T07:52:39Z
OpenJPEG 2.3.0 has a NULL pointer dereference for "red" in the imagetopnm function of jp2/convert.c	Medium	security	JFrog	debian:stretch:openjpeg2	< 2.1.2-1.1+deb9u3	>= 2.1.2-1.1+deb9u3	2019-11-14T07:52:39Z
An invalid memory address dereference was discovered in dwfl_segment_report_module.c in libdwfl in elfutils through v0.174. The vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file, as demonstrated by consider_notes.	Medium	security	JFrog	debian:stretch:elfutils	All Versions		2019-11-14T07:52:39Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The TIFFSetProfiles function in coders/tiff.c in ImageMagick 7.0.6 has incorrect expectations about whether LibTIFF TIFFGetField return values imply that data validation has occurred, which allows remote attackers to cause a denial of service (use-after-free after an invalid call to TIFFSetField, and application crash) via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:10Z
An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31. An invalid memory address dereference was discovered in read_reloc in reloc.c. The vulnerability causes a segmentation fault and application crash, which leads to denial of service, as demonstrated by objdump, because of missing _bfd_clear_contents bounds checking.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:39Z
A SIGFPE is raised in the function box_blur_line of rsvg-filter.c in GNOME librsvg 2.40.17 during an attempted parse of a crafted SVG file, because of incorrect protection against division by zero.	Medium	security	JFrog	debian:stretch:librsvg	All Versions		2019-11-14T07:56:02Z
An issue was discovered in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there is a stack consumption problem caused by recursive stack frames: cplus_demangle_type, d_bare_function_type, d_function_type.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:39Z
makeMultiView.cpp in exrmultiview in OpenEXR 2.3.0 has an out-of-bounds write, leading to an assertion failure or possibly unspecified other impact.	Medium	security	JFrog	debian:stretch:openexr	All Versions		2019-11-14T07:52:39Z
OpenEXR 2.3.0 has a memory leak in ThreadPool in IlmBase/IlmThread/IlmThreadPool.cpp, as demonstrated by exrmultiview.	Medium	security	JFrog	debian:stretch:openexr	All Versions		2019-11-14T07:52:39Z
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.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:39Z
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.	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:52:57Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
Divide-by-zero vulnerabilities in the function arlib_add_symbols() in arlib.c in elfutils 0.174 allow remote attackers to cause a denial of service (application crash) with a crafted ELF file, as demonstrated by eu-ranlib, because a zero sh_entsize is mishandled.	Medium	security	JFrog	debian:stretch:elfutils	All Versions		2019-11-14T07:52:39Z
expat 2.1.0 and earlier does not properly handle entities expansion unless an application developer uses the XML_SetEntityDeclHandler function, which allows remote attackers to cause a denial of service (resource consumption), send HTTP requests to intranet servers, or read arbitrary files via a crafted XML document, aka an XML External Entity (XXE) issue. NOTE: it could be argued that because expat already provides the ability to disable external entity expansion, the responsibility for resolving this issue lies with application developers; according to this argument, this entry should be REJECTed, and each affected application would need its own CVE.	Medium	security	JFrog	debian:stretch:expat	All Versions		2019-11-14T07:53:53Z
When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the WriteHISTOGRAMImage() function in coders/histogram.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:02Z
The process_version_sections function in readelf.c in GNU Binutils 2.29 allows attackers to cause a denial of service (Integer Overflow, and hang because of a time-consuming loop) or possibly have unspecified other impact via a crafted binary file with invalid values of ent.vn_next, during "readelf -a" execution.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
There is a memory leak in the function WriteMSLImage of coders/msl.c in ImageMagick 7.0.8-13 Q16, and the function ProcessMSLScript of coders/msl.c in GraphicsMagick before 1.3.31.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:39Z
An Invalid Memory Address Dereference exists in the function elf_end in libelf in elfutils through v0.174. Although eu-size is intended to support ar files inside ar files, handle_ar in size.c closes the outer ar file before handling all inner entries. The vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file.	Medium	security	JFrog	debian:stretch:elfutils	All Versions		2019-11-14T07:52:39Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The ReadCAPTIONImage function in coders/caption.c in ImageMagick 7.0.7-3 allows remote attackers to cause a denial of service (infinite loop) via a crafted font file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:10Z
An issue was discovered in elf_link_input_bfd in elflink.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31. There is a NULL pointer dereference in elf_link_input_bfd when used for finding STT_TLS symbols without any TLS section. A specially crafted ELF allows remote attackers to cause a denial of service, as demonstrated by ld.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:39Z
A heap-based buffer over-read issue was discovered in the function sec_merge_hash_lookup in merge.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31, because _bfd_add_merge_section mishandles section merges when size is not a multiple of entsize. A specially crafted ELF allows remote attackers to cause a denial of service, as demonstrated by ld.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:39Z
When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the WriteJP2Image() function in coders/jp2.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:02Z
ImageMagick 7.0.6-6 has a memory leak vulnerability in ReadXCFImage in coders/xcf.c via a crafted xcf image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:10Z
An issue was discovered in the merge_strings function in merge.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31. There is a NULL pointer dereference in _bfd_add_merge_section when attempting to merge sections with large alignments. A specially crafted ELF allows remote attackers to cause a denial of service, as demonstrated by ld.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:40Z
load_specific_debug_section in objdump.c in GNU Binutils through 2.31.1 contains an integer overflow vulnerability that can trigger a heap-based buffer overflow via a crafted section size.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:45Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
GNU Binutils 2.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to the byte_get_little_endian function in elfcomm.c, the get_unwind_section_word function in readelf.c, and ARM unwind information that contains invalid word offsets.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:55Z
An issue was discovered in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31. There is a stack consumption vulnerability resulting from infinite recursion in the functions next_is_type_qual() and cplus_demangle_type() in cp-demangle.c. Remote attackers could leverage this vulnerability to cause a denial-of-service via an ELF file, as demonstrated by nm.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:40Z
ImageMagick version 7.0.7-2 contains a memory leak in ReadYUVImage in coders/yuv.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:10Z
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.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:03Z
In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.	Medium	security	JFrog	debian:stretch:openssh	All Versions		2019-11-14T07:52:45Z
The pe_print_idata function in peXXigen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles HintName vector entries, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted PE file, related to the bfd_getl16 function.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
An issue was discovered in LibTIFF 4.0.9. There is a NULL pointer dereference in the function LZWDecode in the file tif_lzw.c.	Medium	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:52:40Z
** DISPUTED ** png_create_info_struct in png.c in libpng 1.6.36 has a memory leak, as demonstrated by pngcp. NOTE: a third party has stated "I don't think it is libpng's job to free this buffer."	Medium	security	JFrog	debian:stretch:libpng1.6	All Versions		2019-11-14T07:52:45Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in ReadOneMNGImage in coders/png.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:10Z
The string component in the GNU C Library (aka glibc or libc6) through 2.28, when running on the x32 architecture, incorrectly attempts to use a 64-bit register for size_t in assembly codes, which can lead to a segmentation fault or possibly unspecified other impact, as demonstrated by a crash in __memmove_avx_unaligned_erms in sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S during a memcpy.	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:52:46Z
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.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:03Z
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.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:46Z
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.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:03Z
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.	Medium	security	JFrog	debian:stretch:libwmf	All Versions		2019-11-14T07:55:40Z
When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the ReadOnePNGImage() function in coders/png.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:02Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, interpret a -1 value as a sorting count instead of an error flag, which allows remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
An issue was discovered in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31. There is a stack consumption vulnerability resulting from infinite recursion in the functions d_name(), d_encoding(), and d_local_name() in cp-demangle.c. Remote attackers could leverage this vulnerability to cause a denial-of-service via an ELF file, as demonstrated by nm.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:40Z
A flaw was found in the Linux kernel in the function hid_debug_events_read() in drivers/hid/hid-debug.c file which may enter an infinite loop with certain parameters passed from a userspace. A local privileged user ("root") can cause a system lock up and a denial of service. Versions from v4.18 and newer are vulnerable.	Medium	security	JFrog	debian:stretch:linux	< 4.9.161-1	>= 4.9.161-1	2019-11-14T07:52:46Z
libjpeg-turbo 1.5.2 has a NULL Pointer Dereference in jdpostct.c and jquant1.c via a crafted JPEG file.	Medium	security	JFrog	debian:stretch:libjpeg-turbo	All Versions		2019-11-14T07:56:11Z
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	Medium	security	JFrog	debian:stretch:mariadb-10.1	< 10.1.38-0+deb9u1	>= 10.1.38-0+deb9u1	2019-11-14T07:52:46Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The DNS stub resolver in the GNU C Library (aka glibc or libc6) before version 2.26, when EDNS support is enabled, will solicit large UDP responses from name servers, potentially simplifying off-path DNS spoofing attacks due to IP fragmentation.	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:56:04Z
DISPUTED An attempted excessive memory allocation was discovered in the function read_long_names in elf_begin.c in libelf in elfutils 0.174. Remote attackers could leverage this vulnerability to cause a denial-of-service via crafted elf input, which leads to an out-of-memory exception. NOTE: The maintainers believe this is not a real issue, but instead a "warning caused by ASAN because the allocation is big. By setting ASAN_OPTIONS=allocator_may_return_null=1 and running the reproducer, nothing happens."	Medium	security	JFrog	debian:stretch:elfutils	All Versions		2019-11-14T07:52:47Z
_bfd_dwarf2_cleanup_debug_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (memory leak) via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:11Z
In OpenJPEG 2.3.0, there is an integer overflow vulnerability in the opj_t1_encode_cblks function (openjp2/t1.c). Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:56:20Z
In ImageMagick before 7.0.8-25, a memory leak exists in ReadSIXELImage in coders/sixel.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:47Z
ReadPSDImage in coders/psd.c in ImageMagick 7.0.7-6 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, related to "Conditional jump or move depends on uninitialised value(s)."	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:11Z
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.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:52:47Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
An integer overflow in xmlmemory.c in libxml2 before 2.9.5, as used in Google Chrome prior to 62.0.3202.62 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted XML file.	Medium	security	JFrog	debian:stretch:libxml2	All Versions		2019-11-14T07:56:12Z
ImageMagick 7.0.6-2 has a memory leak vulnerability in WritePALMImage in coders/palm.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:05Z
In LibTIFF 4.0.9, there is a NULL pointer dereference in the TIFFWriteDirectorySec function in tif_dirwrite.c that will lead to a denial of service attack, as demonstrated by tiffset.	Medium	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:52:40Z
In elfutils 0.175, a negative-sized memcpy is attempted in elf_cvt_note in libelf/note_xlate.h because of an incorrect overflow check. Crafted elf input causes a segmentation fault, leading to denial of service (program crash).	Medium	security	JFrog	debian:stretch:elfutils	All Versions		2019-11-14T07:52:47Z
The evax_bfd_print_emh function in vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:04Z
An Invalid Address dereference was discovered in TIFFWriteDirectoryTagTransferfunction in libtiff/tif_dirwrite.c in LibTIFF 4.0.10, affecting the cpSeparateBufToContigBuf function in tiffcp.c. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted tiff file. This is different from CVE-2018-12900.	Medium	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:52:48Z
The iconv program in the GNU C Library (aka glibc or libc6) 2.25 and earlier, when invoked with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:55:49Z
read_formatted_entries in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite loop) via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
In the Linux kernel through 4.19.6, a local user could exploit a use-after-free in the ALSA driver by supplying a malicious USB Sound device (with zero interfaces) that is mishandled in usb_audio_probe in sound/usb/card.c.	Medium	security	JFrog	debian:stretch:linux	< 4.9.161-1	>= 4.9.161-1	2019-11-14T07:52:42Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
** DISPUTED ** 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.	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:52:49Z
The Linux kernel, when using IPv6, allows remote attackers to determine whether a host is sniffing the network by sending an ICMPv6 Echo Request to a multicast address and determining whether an Echo Reply is sent, as demonstrated by thcping.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:53:58Z
An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an attempted excessive memory allocation in elf_read_notes in elf.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:49Z
** DISPUTED ** 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.	Medium	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:56:14Z
An issue was discovered in ImageMagick 6.9.7. A specially crafted webp file could lead to a file-descriptor leak in libmagickcore (thus, a DoS).	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:55:49Z
When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the lite_font_map() function in coders/wmf.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:02Z
The pe_bfd_read_buildid function in peicode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not validate size and offset values in the data dictionary, which allows remote attackers to cause a denial of service (segmentation violation and application crash) or possibly have unspecified other impact via a crafted PE file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:14Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
OpenSSL 0.9.8i on the Gaisler Research LEON3 SoC on the Xilinx Virtex-II Pro FPGA uses a Fixed Width Exponentiation (FWE) algorithm for certain signature calculations, and does not verify the signature before providing it to a caller, which makes it easier for physically proximate attackers to determine the private key via a modified supply voltage for the microprocessor, related to a "fault-based attack."	Medium	security	JFrog	debian:stretch:openssl	All Versions		2019-11-14T07:54:38Z
An infinite loop vulnerability in tiftoimage that results in heap buffer overflow in convert_32s_C1P1 was found in openjpeg 2.1.2.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:55:42Z
process_debug_info in dwarf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite loop) via a crafted ELF file that contains a negative size value in a CU structure.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
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.	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:52:49Z
sshd in OpenSSH 4 on Debian GNU/Linux, and the 20070303 OpenSSH snapshot, allows remote authenticated users to obtain access to arbitrary SELinux roles by appending a :/ (colon slash) sequence, followed by the role name, to the username.	Medium	security	JFrog	debian:stretch:openssh	All Versions		2019-11-14T07:55:13Z
An issue was discovered in GNU Binutils 2.32. It is a heap-based buffer overflow in process_mips_specific in readelf.c via a malformed MIPS option section.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:49Z
The aout_get_external_symbols function in aoutx.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, allows remote attackers to cause a denial of service (slurp_symtab invalid free and application crash) or possibly have unspecified other impact via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:15Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
ChaCha20-Poly1305 is an AEAD cipher, and requires a unique nonce input for every encryption operation. RFC 7539 specifies that the nonce value (IV) should be 96 bits (12 bytes). OpenSSL allows a variable nonce length and front pads the nonce with 0 bytes if it is less than 12 bytes. However it also incorrectly allows a nonce to be set of up to 16 bytes. In this case only the last 12 bytes are significant and any additional leading bytes are ignored. It is a requirement of using this cipher that nonce values are unique. Messages encrypted using a reused nonce value are susceptible to serious confidentiality and integrity attacks. If an application changes the default nonce length to be longer than 12 bytes and then makes a change to the leading bytes of the nonce expecting the new value to be a new unique nonce then such an application could inadvertently encrypt messages with a reused nonce. Additionally the ignored bytes in a long nonce are not covered by the integrity guarantee of this cipher. Any application that relies on the integrity of these ignored leading bytes of a long nonce may be further affected. Any OpenSSL internal use of this cipher, including in SSL/TLS, is safe because no such use sets such a long nonce value. However user applications that use this cipher directly and set a non-default nonce length to be longer than 12 bytes may be vulnerable. OpenSSL versions 1.1.1 and 1.1.0 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1c (Affected 1.1.1-1.1.1b). Fixed in OpenSSL 1.1.0k (Affected 1.1.0-1.1.0j).	Medium	security	JFrog	debian:stretch:openssl	< 1.1.0k-1~deb9u1	>= 1.1.0k-1~deb9u1	2019-11-14T07:52:50Z
ImageMagick 7.0.6-5 has memory leaks in the parse8BIMW and format8BIM functions in coders/meta.c, related to the WriteImage function in MagickCore/constitute.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
The aout_32_swap_std_reloc_out function in aoutx.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils before 2.31, allows remote attackers to cause a denial of service (segmentation fault and application crash) via a crafted file, as demonstrated by objcopy.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:45:01Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The display_debug_frames function in dwarf.c in GNU Binutils 2.29.1 allows remote attackers to cause a denial of service (integer overflow and heap-based buffer over-read, and application crash) or possibly have unspecified other impact via a crafted ELF file, related to print_debug_frame.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:15Z
In ImageMagick before 7.0.8-25, some memory leaks exist in DecodeImage in coders/pcd.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:50Z
gdk-pixbuf-thumbnailer.c in gdk-pixbuf allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors related to printing an error message.	Medium	security	JFrog	debian:stretch:gdk-pixbuf	All Versions		2019-11-14T07:55:50Z
The coff_slurp_line_table function in coffcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, allows remote attackers to cause a denial of service (invalid memory access and application crash) or possibly have unspecified other impact via a crafted PE file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:15Z
An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit signal are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.	Medium	security	JFrog	debian:stretch:libssh2	< 1.7.0-1+deb9u1	>= 1.7.0-1+deb9u1	2019-11-14T07:52:50Z
In ImageMagick 7.0.6-1, a memory leak vulnerability was found in the function ReadPESImage in coders/pes.c, which allows attackers to cause a denial of service, related to ResizeMagickMemory in memory.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SFTP packets with empty payloads are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	Medium	security	JFrog	debian:stretch:libssh2	< 1.7.0-1+deb9u1	>= 1.7.0-1+deb9u1	2019-11-14T07:52:50Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not validate sizes of core notes, which allows remote attackers to cause a denial of service (bfd_getl32 heap-based buffer over-read and application crash) via a crafted object file, related to elfcore_grok_netbsd_procinfo, elfcore_grok_openbsd_procinfo, and elfcore_grok_nto_status.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:15Z
An integer overflow flaw, which could lead to an out of bounds write, was discovered in libssh2 before 1.8.1 in the way keyboard prompt requests are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.	Medium	security	JFrog	debian:stretch:libssh2	< 1.7.0-1+deb9u1	>= 1.7.0-1+deb9u1	2019-11-14T07:52:50Z
An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the _libssh2_packet_require and _libssh2_packet_requirev functions. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	Medium	security	JFrog	debian:stretch:libssh2	< 1.7.0-1+deb9u1	>= 1.7.0-1+deb9u1	2019-11-14T07:52:50Z
The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, allows remote attackers to cause a denial of service (memory access violation) or possibly have unspecified other impact via a COFF binary in which a relocation refers to a location after the end of the to-be-relocated section.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:15Z
The load_debug_section function in readelf.c in GNU Binutils 2.29.1 allows remote attackers to cause a denial of service (invalid memory access and application crash) or possibly have unspecified other impact via an ELF file that lacks section headers.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:16Z
Stack-based buffer overflow in the pcre32_copy_substring function in pcre_get.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (WRITE of size 4) or possibly have unspecified other impact via a crafted file.	Medium	security	JFrog	debian:stretch:pcre3	All Versions		2019-11-14T07:55:50Z
In SQLite 3.27.2, interleaving reads and writes in a single transaction with an fts5 virtual table will lead to a NULL Pointer Dereference in fts5ChunkIterate in sqlite3.c. This is related to ext/fts5/fts5_hash.c and ext/fts5/fts5_index.c.	Medium	security	JFrog	debian:stretch:sqlite3	All Versions		2019-11-14T07:52:50Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The coff_slurp_reloc_table function in coffcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted COFF based file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:16Z
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.	Medium	security	JFrog	debian:stretch:shadow	All Versions		2019-11-14T07:54:44Z
An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils through 2.31. There is a heap-based buffer overflow in bfd_elf32_swap_phdr_in in elfcode.h because the number of program headers is not restricted.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:43Z
In ImageMagick 7.0.8-35 Q16, there is a stack-based buffer overflow in the function PopHexPixel of coders/ps.c, which allows an attacker to cause a denial of service or code execution via a crafted image file.	Medium	security	JFrog	debian:stretch:imagemagick	< 8:6.9.7.4+dfsg-11+deb9u7	>= 8:6.9.7.4+dfsg-11+deb9u7	2019-11-14T07:52:51Z
The dump_relocs_in_section function in objdump.c in GNU Binutils 2.29.1 does not check for reloc count integer overflows, which allows remote attackers to cause a denial of service (excessive memory allocation, or heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted PE file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:16Z
The _bfd_vms_slurp_eeom function in libbfd.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:04Z
decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite loop) via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils through 2.31. There is an integer overflow and infinite loop caused by the IS_CONTAINED_BY_LMA macro in elf.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:43Z
GIT version 2.15.1 and earlier contains a Input Validation Error vulnerability in Client that can result in problems including messing up terminal configuration to RCE. This attack appear to be exploitable via The user must interact with a malicious git server, (or have their traffic modified in a MITM attack).	Medium	security	JFrog	debian:stretch:git	All Versions		2019-11-14T07:56:23Z
WriteEPTImage in coders/ept.c in ImageMagick 7.0.7-25 Q16 allows remote attackers to cause a denial of service (MagickCore/memory.c double free and application crash) or possibly have unspecified other impact via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:23Z
When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the WriteMPCImage() function in coders/mpc.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:02Z
The _bfd_generic_read_minisymbols function in syms.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31, has a memory leak via a crafted ELF file, leading to a denial of service (memory consumption), as demonstrated by nm.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:43Z
In ImageMagick 7.0.6-5, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:05Z
In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadXPMImage in coders/xpm.c, which allows attackers to cause a denial of service via a crafted xpm image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:16Z
ImageMagick 7.0.8-34 has a "use of uninitialized value" vulnerability in the SyncImageSettings function in MagickCore/image.c. This is related to AcquireImage in magick/image.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:56Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
A flaw was found in the Linux kernel's NFS41+ subsystem. NFS41+ shares mounted in different network namespaces at the same time can make bc_svc_process() use wrong back-channel IDs and cause a use-after-free vulnerability. Thus a malicious container user can cause a host kernel memory corruption and a system panic. Due to the nature of the flaw, privilege escalation cannot be fully ruled out.	Medium	security	JFrog	debian:stretch:linux	< 4.9.161-1	>= 4.9.161-1	2019-11-14T07:52:44Z
_bfd_elf_slurp_version_tables in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), 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 ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
binutils version 2.32 and earlier contains a Integer Overflow vulnerability in objdump, bfd_get_dynamic_reloc_upper_bound,bfd_canonicalize_dynamic_reloc that can result in Integer overflow trigger heap overflow. Successful exploitation allows execution of arbitrary code.. This attack appear to be exploitable via Local. This vulnerability appears to have been fixed in after commit 3a551c7a1b80fca579461774860574eabfd7f18f.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:44Z
** DISPUTED ** Lib/webbrowser.py in Python through 3.6.3 does not validate strings before launching the program specified by the BROWSER environment variable, which might allow remote attackers to conduct argument-injection attacks via a crafted URL. NOTE: a software maintainer indicates that exploitation is impossible because the code relies on subprocess.Popen and the default shell=False setting.	Medium	security	JFrog	debian:stretch:python2.7	All Versions		2019-11-14T07:56:16Z
In systemd before v242-rc4, it was discovered that pam_systemd does not properly sanitize the environment before using the XDG_SEAT variable. It is possible for an attacker, in some particular configurations, to set a XDG_SEAT environment variable which allows for commands to be checked against polkit policies using the "allow_active" element rather than "allow_any".	Medium	security	JFrog	debian:stretch:systemd	< 232-25+deb9u11	>= 232-25+deb9u11	2019-11-14T07:52:52Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
SQLite before 3.25.3, when the FTS3 extension is enabled, encounters an integer overflow (and resultant buffer overflow) for FTS3 queries that occur after crafted changes to FTS3 shadow tables, allowing remote attackers to execute arbitrary code by leveraging the ability to run arbitrary SQL statements (such as in certain WebSQL use cases), aka Magellan.	Medium	security	JFrog	debian:stretch:sqlite3	All Versions		2019-11-14T07:52:44Z
In OpenEXR 2.2.0, an invalid write of size 2 in the = operator function in half.h could cause the application to crash or execute arbitrary code.	Medium	security	JFrog	debian:stretch:openexr	All Versions		2019-11-14T07:55:56Z
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.	Medium	security	JFrog	debian:stretch:jbigkit	All Versions		2019-11-14T07:56:03Z
decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles a length calculation, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to read_1_byte.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
avahi-daemon in Avahi through 0.6.32 and 0.7 inadvertently responds to IPv6 unicast queries with source addresses that are not on-link, which allows remote attackers to cause a denial of service (traffic amplification) and may cause information leakage by obtaining potentially sensitive information from the responding device via port-5353 UDP packets. NOTE: this may overlap CVE-2015-2809.	Medium	security	JFrog	debian:stretch:avahi	All Versions		2019-11-14T07:55:54Z
A flaw was found in Mercurial before 4.9. It was possible to use symlinks and subrepositories to defeat Mercurial's path-checking logic and write files outside a repository.	Medium	security	JFrog	debian:stretch:mercurial	All Versions		2019-11-14T07:52:52Z
ImageMagick 7.0.8-34 has a memory leak vulnerability in the WriteDPXImage function in coders/dpx.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:56Z
scan_unit_for_symbols in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadPICTImage in coders/pict.c, which allows attackers to cause a denial of service via a crafted PICT image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z
The Linux kernel 4.14.67 mishandles certain interaction among XFRM Netlink messages, IPPROTO_AH packets, and IPPROTO_IP packets, which allows local users to cause a denial of service (memory consumption and system hang) by leveraging root access to execute crafted applications, as demonstrated on CentOS 7.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:52Z
When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the ReadMATImage() function in coders/mat.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:03Z
GnuPG version 2.1.12 - 2.2.11 contains a Cross ite Request Forgery (CSRF) vulnerability in dirmngr that can result in Attacker controlled CSRF, Information Disclosure, DoS. This attack appear to be exploitable via Victim must perform a WKD request, e.g. enter an email address in the composer window of Thunderbird/Enigmail. This vulnerability appears to have been fixed in after commit 4a4bb874f63741026bd26264c43bb32b1099f060.	Medium	security	JFrog	debian:stretch:gnupg2	All Versions		2019-11-14T07:52:44Z
Modules/_pickle.c in Python before 3.7.1 has an integer overflow via a large LONG_BINPUT value that is mishandled during a "resize to twice the size" attempt. This issue might cause memory exhaustion, but is only relevant if the pickle format is used for serializing tens or hundreds of gigabytes of data.	Medium	security	JFrog	debian:stretch:python3.5	All Versions		2019-11-14T07:52:44Z
It was discovered that a systemd service that uses DynamicUser property can get new privileges through the execution of SUID binaries, which would allow to create binaries owned by the service transient group with the setgid bit set. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the GID will be recycled.	Medium	security	JFrog	debian:stretch:systemd	All Versions		2019-11-14T07:52:53Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
Division-by-zero vulnerabilities in the functions pi_next_pcrl, pi_next_cprl, and pi_next_rpcl in openmj2/pi.c in OpenJPEG through 2.3.0 allow remote attackers to cause a denial of service (application crash).	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:52:56Z
In ImageMagick 7.0.8-43 Q16, there is a heap-based buffer over-read in the function WriteTIFFImage of coders/tiff.c, which allows an attacker to cause a denial of service or possibly information disclosure via a crafted image file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:53Z
ImageMagick 7.0.7-1 and older version are vulnerable to null pointer dereference in the MagickCore component and might lead to denial of service	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z
The coredump implementation in the Linux kernel before 5.0.10 does not use locking or other mechanisms to prevent vma layout or vma flags changes while it runs, which allows local users to obtain sensitive information, cause a denial of service, or possibly have unspecified other impact by triggering a race condition with mmget_not_zero or get_task_mm calls. This is related to fs/userfaultfd.c, mm/mmap.c, fs/proc/task_mmu.c, and drivers/infiniband/core/uverbs_main.c.	Medium	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u3	>= 4.9.168-1+deb9u3	2019-11-14T07:52:53Z
The ReadPICTImage function in coders/pict.c in ImageMagick 7.0.6-3 allows attackers to cause a denial of service (memory leak) via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:05Z
An integer overflow vulnerability was found in tiftoimage function in openjpeg 2.1.2, resulting in heap buffer overflow.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:55:43Z
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.	Medium	security	JFrog	debian:stretch:openexr	All Versions		2019-11-14T07:56:10Z
In coders/bmp.c in ImageMagick before 7.0.8-16, an input file can result in an infinite loop and hang, with high CPU and memory consumption. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted file.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:44Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-21, there is a stack-based buffer over-read in WriteWEBPImage in coders/webp.c, related to a WEBP_DECODER_ABI_VERSION check.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z
In ImageMagick 7.0.6-2, a memory leak vulnerability was found in the function ReadOneJNGImage in coders/png.c, which allows attackers to cause a denial of service.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
The fill_input_buffer function in jdatasrc.c in libjpeg-turbo 1.5.1 allows remote attackers to cause a denial of service (invalid memory access and application crash) or possibly have unspecified other impact via a crafted jpg file.	Medium	security	JFrog	debian:stretch:libjpeg-turbo	All Versions		2019-11-14T07:42:14Z
The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandle the failure of a certain canonicalization step, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
In ImageMagick 7.0.6-6, a memory exhaustion vulnerability was found in the function format8BIM, which allows attackers to cause a denial of service.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:53Z
In ImageMagick 7.0.6-3, a memory leak vulnerability was found in the function ReadOneJNGImage in coders/png.c, which allows attackers to cause a denial of service.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
readelf.c in GNU Binutils 2017-04-12 has a "cannot be represented in type long" issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:55Z
Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf	Medium	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u2	>= 4.9.168-1+deb9u2	2019-11-14T07:52:53Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In OpenJPEG 2.3.0, there is excessive iteration in the opj_t1_encode_cblks function of openjp2/t1.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file.	Medium	security	JFrog	debian:stretch:openjpeg2	< 2.1.2-1.1+deb9u3	>= 2.1.2-1.1+deb9u3	2019-11-14T07:56:21Z
In ImageMagick 7.0.7-16 Q16, a memory leak vulnerability was found in the function GetImagePixelCache in magick/cache.c, which allows attackers to cause a denial of service via a crafted MNG image file that is processed by ReadOneMNGImage.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:17Z
ImageMagick 7.0.6-2 has a memory leak vulnerability in WriteCALSImage in coders/cals.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
Microarchitectural Fill Buffer Data Sampling (MFBDS): Fill buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf	Medium	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u2	>= 4.9.168-1+deb9u2	2019-11-14T07:52:53Z
An issue was discovered in the Linux kernel before 4.18.7. In block/blk-core.c, there is an __blk_drain_queue() use-after-free because a certain error case is mishandled.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:58Z
A heap buffer overflow in the TFTP receiving code allows for DoS or arbitrary code execution in libcurl versions 7.19.4 through 7.64.1.	Medium	security	JFrog	debian:stretch:curl	All Versions		2019-11-14T07:52:54Z
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.	Medium	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:54:03Z
readelf.c in GNU Binutils 2017-04-12 has a "shift exponent too large for type unsigned long" issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:55:55Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
In GNU Binutils 2.31.1, there is a use-after-free in the error function in elfcomm.c when called from the process_archive function in readelf.c via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:44Z
** DISPUTED ** An issue was discovered in ip_ra_control in net/ipv4/ip_sockglue.c in the Linux kernel through 5.1.5. There is an unchecked kmalloc of new_ra, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). NOTE: this is disputed because new_ra is never used if it is NULL.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:55Z
The jQuery framework exchanges data using JavaScript Object Notation (JSON) without an associated protection scheme, which allows remote attackers to obtain the data via a web page that retrieves the data through a URL in the SRC attribute of a SCRIPT element and captures the data using other JavaScript code, aka "JavaScript Hijacking."	Medium	security	JFrog	debian:stretch:jquery	All Versions		2019-11-14T07:54:24Z
ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in ReadEnhMetaFile in coders/emf.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:10Z
A NULL pointer dereference was discovered in elf_link_add_object_symbols in elflink.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31.1. This occurs for a crafted ET_DYN with no program headers. A specially crafted ELF file allows remote attackers to cause a denial of service, as demonstrated by ld.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:44Z
** DISPUTED ** An issue was discovered in drm_load_edid_firmware in drivers/gpu/drm/drm_edid_load.c in the Linux kernel through 5.1.5. There is an unchecked kstrdup of fwstr, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). NOTE: The vendor disputes this issues as not being a vulnerability because kstrdup() returning NULL is handled sufficiently and there is no chance for a NULL pointer dereference.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:55Z
ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadDCMImage in coders\dcm.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
** DISPUTED ** An issue was discovered in ip6_ra_control in net/ipv6/ipv6_sockglue.c in the Linux kernel through 5.1.5. There is an unchecked kmalloc of new_ra, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). NOTE: This has been disputed as not an issue.	Medium	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:55Z
In ImageMagick 7.0.6-3, a memory leak vulnerability was found in the function ReadOneMNGImage in coders/png.c, which allows attackers to cause a denial of service.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:04Z
ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of a misplaced assignment.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, has a memory leak via a crafted string, leading to a denial of service (memory consumption), as demonstrated by cxxfilt, a related issue to CVE-2018-12698.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:44Z
find_abstract_instance_name in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite recursion and application crash) via a crafted ELF file.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:56:10Z
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.	Medium	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:44Z
ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of off-by-one errors.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:57Z
ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in PDFDelegateMessage in coders/pdf.c.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:10Z
In GNU patch through 2.7.6, the following of symlinks is mishandled in certain cases other than input files. This affects inp.c and util.c.	Medium	security	JFrog	debian:stretch:patch	< 2.7.5-1+deb9u2	>= 2.7.5-1+deb9u2	2019-11-14T07:52:58Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
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.	Medium	security	JFrog	debian:stretch:openjpeg2	All Versions		2019-11-14T07:53:12Z
The ReadTIFFImage function in coders/tiff.c in ImageMagick 7.0.7-26 Q16 does not properly restrict memory allocation, leading to a heap-based buffer over-read.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:23Z
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.	Medium	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:55:46Z
The ReadMATImage function in coders/mat.c in ImageMagick through 6.9.9-3 and 7.x through 7.0.6-3 has memory leaks involving the quantum_info and clone_info data structures.	Medium	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:56:03Z
An issue was discovered in can_can_gw_rcv in net/can/gw.c in the Linux kernel through 4.19.13. The CAN frame modification rules allow bitwise logical operations that can be also applied to the can_dlc field. The privileged user "root" with CAP_NET_ADMIN can create a CAN frame modification rule that makes the data length code a higher value than the available CAN frame data size. In combination with a configured checksum calculation where the result is stored relatively to the end of the data (e.g. cgw_csum_xor_rel) the tail of the skb (e.g. frag_list pointer in skb_shared_info) can be rewritten which finally can cause a system crash. Because of a missing check, the CAN drivers may write arbitrary content beyond the data registers in the CAN controller's I/O memory when processing can-gw manipulated outgoing frames.	Medium	security	JFrog	debian:stretch:linux	< 4.9.161-1	>= 4.9.161-1	2019-11-14T07:52:44Z
The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of the fincore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.	Low	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u3	>= 4.9.168-1+deb9u3	2019-11-14T07:52:45Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
A heap data infoleak in multiple locations including L2CAP_PARSE_CONF_RSP was found in the Linux kernel before 5.1-rc1.	Low	security	JFrog	debian:stretch:linux	< 4.9.168-1	>= 4.9.168-1	2019-11-14T07:52:45Z
** DISPUTED ** libxml2 2.9.4, when used in recover mode, allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted XML document. NOTE: The maintainer states "I would disagree of a CVE with the Recover parsing option which should only be used for manual recovery at least for XML parser."	Low	security	JFrog	debian:stretch:libxml2	All Versions		2019-11-14T07:55:48Z
A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel before 5.1-rc1.	Low	security	JFrog	debian:stretch:linux	< 4.9.168-1	>= 4.9.168-1	2019-11-14T07:52:45Z
In the GNU C Library (aka glibc or libc6) through 2.29, the memcmp function for the x32 architecture can incorrectly return zero (indicating that the inputs are equal) because the RDX most significant bit is mishandled.	Low	security	JFrog	debian:stretch:glibc	All Versions		2019-11-14T07:52:47Z
png_image_free in png.c in libpng 1.6.x before 1.6.37 has a use-after-free because png_image_free_function is called under png_safe_execute.	Low	security	JFrog	debian:stretch:libpng1.6	< 1.6.28-1+deb9u1	>= 1.6.28-1+deb9u1	2019-11-14T07:52:47Z
CVE-2011-4917	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:54:42Z
When apr_time_exp*() or apr_os_exp_time*() functions are invoked with an invalid month field value in Apache Portable Runtime APR 1.6.2 and prior, out of bounds memory may be accessed in converting this value to an apr_time_exp_t value, potentially revealing the contents of a different static heap value or resulting in program termination, and may represent an information disclosure or denial of service vulnerability to applications which call these APR functions with unvalidated external input.	Low	security	JFrog	debian:stretch:apr	All Versions		2019-11-14T07:56:13Z
The KVM implementation in the Linux kernel through 4.20.5 has an Information Leak.	Low	security	JFrog	debian:stretch:linux	< 4.9.161-1	>= 4.9.161-1	2019-11-14T07:52:47Z
Apache Portable Runtime Utility (APR-util) 1.6.0 and prior fail to validate the integrity of SDBM database files used by apr_sdbm*() functions, resulting in a possible out of bound read access. A local user with write access to the database can make a program or process using these functions crash, and cause a denial of service.	Low	security	JFrog	debian:stretch:apr-util	All Versions		2019-11-14T07:56:13Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
** DISPUTED ** In PCRE 8.41, after compiling, a pcretest load test PoC produces a crash overflow in the function match() in pcre_exec.c because of a self-recursive call. NOTE: third parties dispute the relevance of this report, noting that there are options that can be used to limit the amount of stack that is used.	Low	security	JFrog	debian:stretch:pcre3	All Versions		2019-11-14T07:56:14Z
The SCTP socket buffer used by a userspace application is not accounted by the cgroups subsystem. An attacker can use this flaw to cause a denial of service attack. Kernel 3.10.x and 4.18.x branches are believed to be vulnerable.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:50Z
** DISPUTED ** Kernel Samepage Merging (KSM) in the Linux kernel 2.6.32 through 4.x does not prevent use of a write-timing side channel, which allows guest OS users to defeat the ASLR protection mechanism on other guest OS instances via a Cross-VM ASL INtrospection (CAIN) attack. NOTE: the vendor states "Basically if you care about this attack vector, disable deduplication." Share-until-written approaches for memory conservation among mutually untrusting tenants are inherently detectable for information disclosure, and can be classified as potentially misunderstood behaviors rather than vulnerabilities.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:53:21Z
The hidma_chan_stats function in drivers/dma/qcom/hidma_dbg.c in the Linux kernel 4.14.90 allows local users to obtain sensitive address information by reading "callback=" lines in a debugfs file.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:51Z
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.	Low	security	JFrog	debian:stretch:coreutils	All Versions		2019-11-14T07:53:08Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
** DISPUTED ** The Linux kernel through 5.0.7, when CONFIG_IA32_AOUT is enabled and ia32_aout is loaded, allows local users to bypass ASLR on setuid a.out programs (if any exist) because install_exec_creds() is called too late in load_aout_binary() in fs/binfmt_aout.c, and thus the ptrace_may_access() check has a race condition when reading /proc/pid/stat. NOTE: the software maintainer disputes that this is a vulnerability because ASLR for a.out format executables has never been supported.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:52Z
CVE-2019-9500	Low	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u3	>= 4.9.168-1+deb9u3	2019-11-14T07:52:52Z
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.	Low	security	JFrog	debian:stretch:coreutils	All Versions		2019-11-14T07:56:17Z
An off-by-one read vulnerability was discovered in ImageMagick before version 7.0.7-28 in the formatIPTCfromBuffer function in coders/meta.c. A local attacker may use this flaw to read beyond the end of the buffer or to crash the program.	Low	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:52:53Z
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	Low	security	JFrog	debian:stretch:mariadb-10.1	All Versions		2019-11-14T07:52:53Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
A vulnerability was found in PostgreSQL versions 11.x up to excluding 11.3, 10.x up to excluding 10.8, 9.6.x up to, excluding 9.6.13, 9.5.x up to, excluding 9.5.17. PostgreSQL maintains column statistics for tables. Certain statistics, such as histograms and lists of most common values, contain values taken from the column. PostgreSQL does not evaluate row security policies before consulting those statistics during query planning; an attacker can exploit this to read the most common values of certain columns. Affected columns are those for which the attacker has SELECT privilege and for which, in an ordinary query, row-level security prunes the set of rows visible to the attacker.	Low	security	JFrog	debian:stretch:postgresql-9.6	< 9.6.13-0+deb9u1	>= 9.6.13-0+deb9u1	2019-11-14T07:52:53Z
The do_hidp_sock_ioctl function in net/bluetooth/hidp/sock.c in the Linux kernel before 5.0.15 allows a local user to obtain potentially sensitive information from kernel stack memory via a HIDPCONNADD command, because a name field may not end with a '\0' character.	Low	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u3	>= 4.9.168-1+deb9u3	2019-11-14T07:52:53Z
fs/ext4/extents.c in the Linux kernel through 5.1.2 does not zero out the unused memory region in the extent tree block, which might allow local users to obtain sensitive information by reading uninitialized data in the filesystem.	Low	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u3	>= 4.9.168-1+deb9u3	2019-11-14T07:52:53Z
A flaw was found in the Linux kernel's freescale hypervisor manager implementation, kernel versions 5.0.x up to, excluding 5.0.17. A parameter passed to an ioctl was incorrectly validated and used in size calculations for the page size calculation. An attacker can use this flaw to crash the system, corrupt memory, or create other adverse security affects.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:55Z
The acpi_ns_evaluate() function in drivers/acpi/acpica/nseval.c in the Linux kernel through 4.12.9 does not flush the operand cache and causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism (in the kernel through 4.9) via a crafted ACPI table.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:56:04Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The print_binder_transaction_ilocked function in drivers/android/binder.c in the Linux kernel 4.14.90 allows local users to obtain sensitive address information by reading "*from *code *flags" lines in a debugfs file.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:55Z
The print_binder_ref_olocked function in drivers/android/binder.c in the Linux kernel 4.14.90 allows local users to obtain sensitive address information by reading " ref *desc *node" lines in a debugfs file.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:55Z
DISPUTED An issue was discovered in the efi subsystem in the Linux kernel through 5.1.5. phys_efi_set_virtual_address_map in arch/x86/platform/efi/efi.c and efi_call_phys_prolog in arch/x86/platform/efi/efi_64.c mishandle memory allocation failures. NOTE: This id is disputed as not being an issue because ?All the code touched by the referenced commit runs only at boot, before any user processes are started. Therefore, there is no possibility for an unprivileged user to control it.?.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:55Z
dbus before 1.10.28, 1.12.x before 1.12.16, and 1.13.x before 1.13.12, as used in DBusServer in Canonical Upstart in Ubuntu 14.04 (and in some, less common, uses of dbus-daemon), allows cookie spoofing because of symlink mishandling in the reference implementation of DBUS_COOKIE_SHA1 in the libdbus library. (This only affects the DBUS_COOKIE_SHA1 authentication mechanism.) A malicious client with write access to its own home directory could manipulate a ~/.dbus-keyrings symlink to cause a DBusServer with a different uid to read and write in unintended locations. In the worst case, this could result in the DBusServer reusing a cookie that is known to the malicious client, and treating that cookie as evidence that a subsequent client connection came from an attacker-chosen uid, allowing authentication bypass.	Low	security	JFrog	debian:stretch:dbus	< 1.10.28-0+deb9u1	>= 1.10.28-0+deb9u1	2019-11-14T07:52:56Z
An issue was discovered in the Linux kernel before 5.0. The function __mdiobus_register() in drivers/net/phy/mdio_bus.c calls put_device(), which will trigger a fixed_mdio_bus_init use-after-free. This will cause a denial of service.	Low	security	JFrog	debian:stretch:linux	< 4.9.168-1	>= 4.9.168-1	2019-11-14T07:52:56Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
CVE-2011-3374	Low	security	JFrog	debian:stretch:apt	All Versions		2019-11-14T07:54:13Z
An issue was discovered in OpenLDAP 2.x before 2.4.48. When using SASL authentication and session encryption, and relying on the SASL security layers in slapd access controls, it is possible to obtain access that would otherwise be denied via a simple bind for any identity covered in those ACLs. After the first SASL bind is completed, the sasl_ssf value is retained for all new non-SASL connections. Depending on the ACL configuration, this can affect different types of operations (searches, modifications, etc.). In other words, a successful authorization step completed by one user affects the authorization requirement for a different user.	Low	security	JFrog	debian:stretch:openldap	All Versions		2019-11-14T07:52:58Z
An issue was discovered in the server in OpenLDAP before 2.4.48. When the server administrator delegates rootDN (database admin) privileges for certain databases but wants to maintain isolation (e.g., for multi-tenant deployments), slapd does not properly stop a rootDN from requesting authorization as an identity from another database during a SASL bind or with a proxyAuthz (RFC 4370) control. (It is not a common configuration to deploy a system where the server administrator and a DB administrator enjoy different levels of trust.)	Low	security	JFrog	debian:stretch:openldap	All Versions		2019-11-14T07:52:58Z
In the Linux kernel before 5.2.3, drivers/block/floppy.c allows a denial of service by setup_format_params division-by-zero. Two consecutive ioctls can trigger the bug: the first one should set the drive geometry with .sect and .rate values that make F_SECT_PER_TRACK be zero. Next, the floppy format operation should be called. It can be triggered by an unprivileged local user even when a floppy disk has not been inserted. NOTE: QEMU creates the floppy device by default.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:58Z
apply_relocations in readelf.c in GNU Binutils 2.32 contains an integer overflow that allows attackers to trigger a write access violation (in byte_put_little_endian function in elfcomm.c) via an ELF file, as demonstrated by readelf.	Low	security	JFrog	debian:stretch:binutils	All Versions		2019-11-14T07:52:58Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The Serial Attached SCSI (SAS) implementation in the Linux kernel through 4.15.9 mishandles a mutex within libsas, which allows local users to cause a denial of service (deadlock) by triggering certain error-handling code.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:56:23Z
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	Low	security	JFrog	debian:stretch:mariadb-10.1	All Versions		2019-11-14T07:52:58Z
The unimac_mdio_probe function in drivers/net/phy/mdio-bcm-unimac.c in the Linux kernel through 4.15.8 does not validate certain resource availability, which allows local users to cause a denial of service (NULL pointer dereference).	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:56:23Z
CVE-2012-3878	Low	security	JFrog	debian:stretch:perl	All Versions		2019-11-14T07:39:45Z
CVE-2008-2544	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:53:39Z
The acpi_ps_complete_final_op() function in drivers/acpi/acpica/psobject.c in the Linux kernel through 4.12.9 does not flush the node and node_ext caches and causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism (in the kernel through 4.9) via a crafted ACPI table.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:56:07Z
The krb5-send-pr script in the kerberos5 (krb5) package in Trustix Secure Linux 1.5 through 2.1, and possibly other operating systems, allows local users to overwrite files via a symlink attack on temporary files.	Low	security	JFrog	debian:stretch:krb5	All Versions		2019-11-14T07:53:18Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The process scheduler in the Linux kernel 2.6.16 gives preference to "interactive" processes that perform voluntary sleeps, which allows local users to cause a denial of service (CPU consumption), as described in "Secretly Monopolizing the CPU Without Superuser Privileges."	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:53:01Z
Xen allows guest OS users to obtain sensitive information from uninitialized locations in host OS kernel memory by not enabling memory and I/O decoding control bits. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-0777.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:54:28Z
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.	Low	security	JFrog	debian:stretch:openldap	All Versions		2019-11-14T07:56:08Z
An information disclosure vulnerability in the kernel trace subsystem could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34277115.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:34Z
CVE-2013-4235	Low	security	JFrog	debian:stretch:shadow	All Versions		2019-11-14T07:54:30Z
The swiotlb_print_info function in lib/swiotlb.c in the Linux kernel through 4.14.14 allows local users to obtain sensitive address information by reading dmesg data from a "software IO TLB" printk call.	Low	security	JFrog	debian:stretch:linux	< 4.9.161-1	>= 4.9.161-1	2019-11-14T07:52:34Z
The pcpu_embed_first_chunk function in mm/percpu.c in the Linux kernel through 4.14.14 allows local users to obtain sensitive address information by reading dmesg data from a "pages/cpu" printk call.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:34Z
The aoedisk_debugfs_show function in drivers/block/aoe/aoeblk.c in the Linux kernel through 4.16.4rc4 allows local users to obtain sensitive address information by reading "ffree: " lines in a debugfs file.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:35Z
CVE-2011-4116	Low	security	JFrog	debian:stretch:perl	All Versions		2019-11-14T07:54:33Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The acpi_ns_terminate() function in drivers/acpi/acpica/nsutils.c in the Linux kernel before 4.12 does not flush the operand cache and causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism (in the kernel through 4.9) via a crafted ACPI table.	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:56:02Z
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.	Low	security	JFrog	debian:stretch:imagemagick	All Versions		2019-11-14T07:54:33Z
CVE-2016-6251	Low	security	JFrog	debian:stretch:shadow	All Versions		2019-11-14T07:40:02Z
A Bleichenbacher type side-channel based padding oracle attack was found in the way nettle handles endian conversion of RSA decrypted PKCS#1 v1.5 data. An attacker who is able to run a process on the same physical core as the victim process, could use this flaw extract plaintext or in some cases downgrade any TLS connections to a vulnerable server.	Low	security	JFrog	debian:stretch:nettle	All Versions		2019-11-14T07:52:42Z
A Bleichenbacher type side-channel based padding oracle attack was found in the way gnutls handles verification of RSA decrypted PKCS#1 v1.5 data. An attacker who is able to run process on the same physical core as the victim process, could use this to extract plaintext or in some cases downgrade any TLS connections to a vulnerable server.	Low	security	JFrog	debian:stretch:gnutls28	All Versions		2019-11-14T07:52:42Z
Avahi version 0.7 contains a Incorrect Access Control vulnerability in avahi-daemon that can result in Traffic reflection and amplification for DDoS attacks.. This attack appear to be exploitable via unicast IP network packet with spoofed source address.	Low	security	JFrog	debian:stretch:avahi	All Versions		2019-11-14T07:44:32Z
The function hso_get_config_data in drivers/net/usb/hso.c in the Linux kernel through 4.19.8 reads if_num from the USB device (as a u8) and uses it to index a small array, resulting in an object out-of-bounds (OOB) read that potentially allows arbitrary read in the kernel address space.	Low	security	JFrog	debian:stretch:linux	< 4.9.161-1	>= 4.9.161-1	2019-11-14T07:52:44Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
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.	Low	security	JFrog	debian:stretch:systemd	All Versions		2019-11-14T07:53:56Z
CVE-2011-4915	Low	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:54:38Z
GNU Tar through 1.30, when --sparse is used, mishandles file shrinkage during read access, which allows local users to cause a denial of service (infinite read loop in sparse_dump_region in sparse.c) by modifying a file that is supposed to be archived by a different user's process (e.g., a system backup running as root).	Low	security	JFrog	debian:stretch:tar	All Versions		2019-11-14T07:52:44Z
A Reachable Assertion issue was discovered in the KDC in MIT Kerberos 5 (aka krb5) before 1.17. If an attacker can obtain a krbtgt ticket using an older encryption type (single-DES, triple-DES, or RC4), the attacker can crash the KDC by making an S4U2Self request.	Low	security	JFrog	debian:stretch:krb5	All Versions		2019-11-14T07:52:44Z
It was discovered systemd does not correctly check the content of PIDFile files before using it to kill processes. When a service is run from an unprivileged user (e.g. User field set in the service file), a local attacker who is able to write to the PIDFile of the mentioned service may use this flaw to trick systemd into killing other services and/or privileged processes. Versions before v237 are vulnerable.	Low	security	JFrog	debian:stretch:systemd	All Versions		2019-11-14T07:52:44Z
CVE-2019-5010	Unknown	security	JFrog	debian:stretch:python2.7	All Versions		2019-11-14T07:52:46Z
CVE-2019-3892	Unknown	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:45:08Z
CVE-2019-9619	Unknown	security	JFrog	debian:stretch:systemd	All Versions		2019-11-14T07:52:51Z
CVE-2019-9503	Unknown	security	JFrog	debian:stretch:linux	< 4.9.168-1+deb9u3	>= 4.9.168-1+deb9u3	2019-11-14T07:52:52Z
GNU patch through 2.7.6 is vulnerable to OS shell command injection that can be exploited by opening a crafted patch file that contains an ed style diff payload with shell metacharacters. The ed editor does not need to be present on the vulnerable system. This is different from CVE-2018-1000156.	Unknown	security	JFrog	debian:stretch:patch	< 2.7.5-1+deb9u2	>= 2.7.5-1+deb9u2	2019-11-14T07:52:58Z
CVE-2019-10207	Unknown	security	JFrog	debian:stretch:linux	All Versions		2019-11-14T07:52:58Z

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
CVE-2018-11782	Unknown	security	JFrog	debian:stretch:subversion	< 1.9.5-1+deb9u4	>= 1.9.5-1+deb9u4	2019-11-14T07:52:58Z
CVE-2019-0203	Unknown	security	JFrog	debian:stretch:subversion	< 1.9.5-1+deb9u4	>= 1.9.5-1+deb9u4	2019-11-14T07:52:58Z
An issue was discovered in LibTIFF 4.0.9. A buffer overflow can occur via an empty fmt argument to unixErrorHandler in tif_unix.c, and it can be exploited (at a minimum) via the following high-level library API functions: TIFFClientOpen, TIFFFdOpen, TIFFRawStripSize, TIFFCheckTile, TIFFComputeStrip, TIFFReadRawTile, TIFFUnRegisterCODEC, and TIFFWriteEncodedTile.	Unknown	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:43:55Z
An issue was discovered in LibTIFF 4.0.9. A buffer overflow vulnerability can occur via an invalid or empty tif argument to TIFFRGBAImageOK in tif_getimage.c, and it can be exploited (at a minimum) via the following high-level library API functions: TIFFReadRGBAImage, TIFFRGBAImageOK, and TIFFRGBAImageBegin.	Unknown	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:43:55Z
An issue was discovered in LibTIFF 4.0.9. A buffer overflow can occur via an invalid or empty tif argument to TIFFWriteBufferSetup in tif_write.c, and it can be exploited (at a minimum) via the following high-level library API function: TIFFWriteTile.	Unknown	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:43:55Z
An issue was discovered in LibTIFF 4.0.9. In TIFFFindField in tif_dirinfo.c, the structure tif is being dereferenced without first checking that the structure is not empty and has the requested fields (tif_foundfield). In the call sequences following from the affected library functions (TIFFVGetField, TIFFVGetFieldDefaulted, TIFFVStripSize, TIFFScanlineSize, TIFFTileSize, TIFFGetFieldDefaulted, and TIFFGetField), this sanitization of the tif structure is never being done and, hence, using them with an invalid or empty tif structure will trigger a buffer overflow, leading to a crash.	Unknown	security	JFrog	debian:stretch:tiff	All Versions		2019-11-14T07:43:55Z