Scan Report: nginx:latest

Scan ID: 19e7b0c7-55b8-4638-80ee-c052130118eb
Scan requested at: 2021-06-30T09:46:01Z
Database time: 2021-06-29T09:51:36Z
Vulnerabilities: defcon1 - 0, critical - 6, high - 38, medium - 40

Attack Vector: Network, Severity: Critical

CVE-2005-2541	
Vers: 1.30+dfsg-6	Fix: n/a
Name: tar Namespace: debian:10 Description: Tar 1.15.1 does not properly warn the user when extracting setuid or setgid files, which may allow local users or remote attackers to gain privileges.	

CVE-2017-9117	
Vers: 4.1.0+git191117-2~deb10u2	Fix: n/a
Name: tiff Namespace: debian:10 Description: In LibTIFF 4.0.7, the program processes BMP images without verifying that biWidth and biHeight in the bitmap-information header match the actual input, leading to a heap-based buffer over-read in bmp2tiff.	

CVE-2018-25012	
Vers: 0.6.1-2+deb10u1	Fix: n/a
Name: libwebp Namespace: debian:10 Description: A flaw was found in libwebp in versions before 1.0.1. An out-of-bounds read was found in function WebPMuxCreateInternal. The highest threat from this vulnerability is to data confidentiality and to the service availability.	

CVE-2019-1010022	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 Description: ** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."	

Scan Report: nginx:latest

Scan ID: 19e7b0c7-55b8-4638-80ee-c052130118eb
Scan requested at: 2021-06-30T09:46:01Z
Database time: 2021-06-29T09:51:36Z
Vulnerabilities: defcon1 - 0, critical - 6, high - 38, medium - 40

CVE-2019-9893	
Vers: 2.3.3-4	Fix: n/a
Name: libseccomp Namespace: debian:10 Description: libseccomp before 2.4.0 did not correctly generate 64-bit syscall argument comparisons using the arithmetic operators (LT, GT, LE, GE), which might able to lead to bypassing seccomp filters and potential privilege escalations.	

CVE-2021-33574	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 Description: The mq_notify function in the GNU C Library (aka glibc) versions 2.32 and 2.33 has a use-after-free. It may use the notification thread attributes object (passed through its struct sigevent parameter) after it has been freed by the caller, leading to a denial of service (application crash) or possibly unspecified other impact.	

Attack Vector: Network, Severity: High

CVE-2011-4116	
Vers: 5.28.1-6+deb10u1	Fix: n/a
Name: perl Namespace: debian:10 Description: _is_safe in the File::Temp module for Perl does not properly handle symlinks.	

CVE-2013-0337	
Vers: 1.21.0-1~buster	Fix: n/a
Name: nginx Namespace: debian:10 Description: The default configuration of nginx, possibly 1.3.13 and earlier, uses world-readable permissions for the (1) access.log and (2) error.log files, which allows local users to obtain sensitive information by reading the files.	

Scan Report: nginx:latest

Scan ID: 19e7b0c7-55b8-4638-80ee-c052130118eb
Scan requested at: 2021-06-30T09:46:01Z
Database time: 2021-06-29T09:51:36Z
Vulnerabilities: defcon1 - 0, critical - 6, high - 38, medium - 40

CVE-2017-11164	
Vers: 2:8.39-12	Fix: n/a
Name: pcre3 Namespace: debian:10 Description: 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.	

CVE-2017-16232	
Vers: 4.1.0+git191117-2~deb10u2	Fix: n/a
Name: tiff Namespace: debian:10 Description: ** 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.	

CVE-2017-16932	
Vers: 2.9.4+dfsg1-7+deb10u2	Fix: n/a
Name: libxml2 Namespace: debian:10 Description: parser.c in libxml2 before 2.9.5 does not prevent infinite recursion in parameter entities.	

CVE-2017-17740	
Vers: 2.4.47+dfsg-3+deb10u6	Fix: n/a
Name: openldap Namespace: debian:10 Description: contrib/slapd-modules/nops/nops.c in OpenLDAP through 2.4.45, when both the nops module and the memberof overlay are enabled, attempts to free a buffer that was allocated on the stack, which allows remote attackers to cause a denial of service (slapd crash) via a member MODDN operation.	

CVE-2017-17973	
Vers: 4.1.0+git191117-2~deb10u2	Fix: n/a
Name: tiff Namespace: debian:10	

Scan Report: nginx:latest

Scan ID: 19e7b0c7-55b8-4638-80ee-c052130118eb
Scan requested at: 2021-06-30T09:46:01Z
Database time: 2021-06-29T09:51:36Z
Vulnerabilities: defcon1 - 0, critical - 6, high - 38, medium - 40

Description: ** 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.

CVE-2017-5563	
Vers: 4.1.0+git191117-2~deb10u2	Fix: n/a
Name: tiff Namespace: debian:10 Description: LibTIFF version 4.0.7 is vulnerable to a heap-based buffer over-read in tif_lzw.c resulting in DoS or code execution via a crafted bmp image to tools/bmp2tiff.	

CVE-2017-6363	
Vers: 2.2.5-5.2	Fix: n/a
Name: libgd2 Namespace: debian:10 Description: ** DISPUTED ** In the GD Graphics Library (aka LibGD) through 2.2.5, there is a heap-based buffer over-read in tiffWriter in gd_tiff.c. NOTE: the vendor says "In my opinion this issue should not have a CVE, since the GD and GD2 formats are documented to be 'obsolete, and should only be used for development and testing purposes.'"	

CVE-2017-7245	
Vers: 2:8.39-12	Fix: n/a
Name: pcre3 Namespace: debian:10 Description: 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.	

CVE-2017-7246	
Vers: 2:8.39-12	Fix: n/a
Name: pcre3 Namespace: debian:10 Description: 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	

Scan Report: nginx:latest

Scan ID: 19e7b0c7-55b8-4638-80ee-c052130118eb
Scan requested at: 2021-06-30T09:46:01Z
Database time: 2021-06-29T09:51:36Z
Vulnerabilities: defcon1 - 0, critical - 6, high - 38, medium - 40

possibly have unspecified other impact via a crafted file.

CVE-2018-11813	
Vers: 1:1.5.2-2+deb10u1	Fix: n/a
Name: libjpeg-turbo Namespace: debian:10 Description: libjpeg 9c has a large loop because read_pixel in rdtarga.c mishandles EOF.	

CVE-2018-12886	
Vers: 8.3.0-6	Fix: n/a
Name: gcc-8 Namespace: debian:10 Description: 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.	

CVE-2018-14550	
Vers: 1.6.36-6	Fix: n/a
Name: libpng1.6 Namespace: debian:10 Description: 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.	

CVE-2018-14553	
Vers: 2.2.5-5.2	Fix: n/a
Name: libgd2 Namespace: debian:10 Description: gdImageClone in gd.c in libgd 2.1.0-rc2 through 2.2.5 has a NULL pointer dereference allowing attackers to crash an application via a specific function call sequence. Only affects PHP when linked with an external libgd (not bundled).	

Scan Report: nginx:latest

Scan ID: 19e7b0c7-55b8-4638-80ee-c052130118eb
Scan requested at: 2021-06-30T09:46:01Z
Database time: 2021-06-29T09:51:36Z
Vulnerabilities: defcon1 - 0, critical - 6, high - 38, medium - 40

CVE-2018-20796	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 Description: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\\1\\1|t1|\\\2537)+' in grep.	

CVE-2018-5709	
Vers: 1.17-3+deb10u1	Fix: n/a
Name: krb5 Namespace: debian:10 Description: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.	

CVE-2018-6829	
Vers: 1.8.4-5+deb10u1	Fix: n/a
Name: libgcrypt20 Namespace: debian:10 Description: cipher/elgamal.c in Libgcrypt through 1.8.2, when used to encrypt messages directly, improperly encodes plaintexts, which allows attackers to obtain sensitive information by reading ciphertext data (i.e., it does not have semantic security in face of a ciphertext-only attack). The Decisional Diffie-Hellman (DDH) assumption does not hold for Libgcrypt's ElGamal implementation.	

CVE-2019-1010023	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 Description: ** DISPUTED ** GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code. NOTE: Upstream comments indicate "this is being treated as a non-security	

Scan Report: nginx:latest

Scan ID: 19e7b0c7-55b8-4638-80ee-c052130118eb
Scan requested at: 2021-06-30T09:46:01Z
Database time: 2021-06-29T09:51:36Z
Vulnerabilities: defcon1 - 0, critical - 6, high - 38, medium - 40

bug and no real threat."

CVE-2019-12290	
Vers: 2.0.5-1+deb10u1	Fix: n/a
Name: libidn2 Namespace: debian:10 Description: GNU libidn2 before 2.2.0 fails to perform the roundtrip checks specified in RFC3490 Section 4.2 when converting A-labels to U-labels. This makes it possible in some circumstances for one domain to impersonate another. By creating a malicious domain that matches a target domain except for the inclusion of certain punycoded Unicode characters (that would be discarded when converted first to a Unicode label and then back to an ASCII label), arbitrary domains can be impersonated.	

CVE-2019-13115	
Vers: 1.8.0-2.1	Fix: n/a
Name: libssh2 Namespace: debian:10 Description: 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.	

CVE-2019-14855	
Vers: 2.2.12-1+deb10u1	Fix: n/a
Name: gnupg2 Namespace: debian:10 Description: A flaw was found in the way certificate signatures could be forged using collisions found in the SHA-1 algorithm. An attacker could use this weakness to create forged certificate signatures. This issue affects GnuPG versions before 2.2.18.	

CVE-2019-15847

Scan Report: nginx:latest

Scan ID: 19e7b0c7-55b8-4638-80ee-c052130118eb
Scan requested at: 2021-06-30T09:46:01Z
Database time: 2021-06-29T09:51:36Z
Vulnerabilities: defcon1 - 0, critical - 6, high - 38, medium - 40

Vers: 8.3.0-6	Fix: n/a
Name: gcc-8 Namespace: debian:10 Description: The POWER9 backend in GNU Compiler Collection (GCC) before version 10 could optimize multiple calls of the __builtin_darn intrinsic into a single call, thus reducing the entropy of the random number generator. This occurred because a volatile operation was not specified. For example, within a single execution of a program, the output of every __builtin_darn() call may be the same.	

CVE-2019-17498	
Vers: 1.8.0-2.1	Fix: n/a
Name: libssh2 Namespace: debian:10 Description: In libssh2 v1.9.0 and earlier versions, the SSH_MSG_DISCONNECT logic in packet.c has an integer overflow in a bounds check, enabling an attacker to specify an arbitrary (out-of-bounds) offset for a subsequent memory read. A crafted 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.	

CVE-2019-17543	
Vers: 1.8.3-1+deb10u1	Fix: n/a
Name: lz4 Namespace: debian:10 Description: LZ4 before 1.9.2 has a heap-based buffer overflow in LZ4_write32 (related to LZ4_compress_destSize), affecting applications that call LZ4_compress_fast with a large input. (This issue can also lead to data corruption.) NOTE: the vendor states "only a few specific / uncommon usages of the API are at risk."	

CVE-2019-20838	
Vers: 2:8.39-12	Fix: n/a
Name: pcre3 Namespace: debian:10 Description: libpcre in PCRE before 8.43 allows a subject buffer over-read in JIT when UTF is disabled, and \X or \R has more than one fixed quantifier, a related issue to CVE-2019-20454.	

Scan Report: nginx:latest

Scan ID: 19e7b0c7-55b8-4638-80ee-c052130118eb
Scan requested at: 2021-06-30T09:46:01Z
Database time: 2021-06-29T09:51:36Z
Vulnerabilities: defcon1 - 0, critical - 6, high - 38, medium - 40

CVE-2019-9192	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 Description: ** 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.	

CVE-2019-9923	
Vers: 1.30+dfsg-6	Fix: n/a
Name: tar Namespace: debian:10 Description: 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.	

CVE-2020-17541	
Vers: 1:1.5.2-2+deb10u1	Fix: n/a
Name: libjpeg-turbo Namespace: debian:10 Description: Libjpeg-turbo all version have a stack-based buffer overflow in the "transform" component. A remote attacker can send a malformed jpeg file to the service and cause arbitrary code execution or denial of service of the target service.	

CVE-2020-6096	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 Description: An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, this memcpy() implementation allows for program execution to continue in	

Scan Report: nginx:latest

Scan ID: 19e7b0c7-55b8-4638-80ee-c052130118eb
Scan requested at: 2021-06-30T09:46:01Z
Database time: 2021-06-29T09:51:36Z
Vulnerabilities: defcon1 - 0, critical - 6, high - 38, medium - 40

scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data.

CVE-2021-22898	
Vers: 7.64.0-4+deb10u2	Fix: n/a
Name: curl Namespace: debian:10 Description: curl 7.7 through 7.76.1 suffers from an information disclosure when the `-t` command line option, known as `CURLOPT_TELNETOPTIONS` in libcurl, is used to send variable=content pairs to TELNET servers. Due to a flaw in the option parser for sending NEW_ENV variables, libcurl could be made to pass on uninitialized data from a stack based buffer to the server, resulting in potentially revealing sensitive internal information to the server using a clear-text network protocol.	

CVE-2021-3326	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 Description: The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid input sequences in the ISO-2022-JP-3 encoding, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.	

Additional Findings

CVE-2007-5686	AV: local	Severity: medium
CVE-2007-6755	AV: network	Severity: medium
CVE-2009-4487	AV: network	Severity: medium
CVE-2010-0928	AV: local	Severity: medium
CVE-2010-4051	AV: network	Severity: medium
CVE-2010-4052	AV: network	Severity: medium
CVE-2010-4756	AV: network	Severity: medium
CVE-2011-3389	AV: network	Severity: medium
CVE-2013-0340	AV: network	Severity: medium
CVE-2013-4235	AV: local	Severity: medium

Scan Report: nginx:latest

Scan ID: 19e7b0c7-55b8-4638-80ee-c052130118eb
Scan requested at: 2021-06-30T09:46:01Z
Database time: 2021-06-29T09:51:36Z
Vulnerabilities: defcon1 - 0, critical - 6, high - 38, medium - 40

CVE-2014-8130	AV: network	Severity: medium
CVE-2015-3276	AV: network	Severity: medium
CVE-2015-9019	AV: network	Severity: medium
CVE-2016-10228	AV: network	Severity: medium
CVE-2016-2781	AV: local	Severity: medium
CVE-2016-9318	AV: network	Severity: medium
CVE-2017-14159	AV: local	Severity: medium
CVE-2017-15232	AV: network	Severity: medium
CVE-2017-16231	AV: local	Severity: medium
CVE-2017-18018	AV: local	Severity: medium
CVE-2017-9937	AV: network	Severity: medium
CVE-2018-1000654	AV: network	Severity: medium
CVE-2018-10126	AV: network	Severity: medium
CVE-2018-14048	AV: network	Severity: medium
CVE-2018-7169	AV: network	Severity: medium
CVE-2019-1010024	AV: network	Severity: medium
CVE-2019-1010025	AV: network	Severity: medium
CVE-2019-13627	AV: local	Severity: medium
CVE-2019-18276	AV: local	Severity: high
CVE-2019-19882	AV: local	Severity: high
CVE-2019-25013	AV: network	Severity: medium
CVE-2019-3843	AV: local	Severity: high
CVE-2019-3844	AV: local	Severity: high
CVE-2019-6129	AV: network	Severity: medium
CVE-2020-10029	AV: local	Severity: medium
CVE-2020-13529	AV: local	Severity: medium
CVE-2020-13776	AV: local	Severity: medium
CVE-2020-14155	AV: network	Severity: medium
CVE-2020-15719	AV: network	Severity: medium
CVE-2020-1751	AV: local	Severity: high
CVE-2020-1752	AV: local	Severity: high
CVE-2020-27618	AV: local	Severity: medium
CVE-2020-35521	AV: network	Severity: medium
CVE-2020-35522	AV: network	Severity: medium

Scan Report: nginx:latest

Scan ID: 19e7b0c7-55b8-4638-80ee-c052130118eb
Scan requested at: 2021-06-30T09:46:01Z
Database time: 2021-06-29T09:51:36Z
Vulnerabilities: defcon1 - 0, critical - 6, high - 38, medium - 40

CVE-2020-36309	AV: network	Severity: medium
CVE-2021-20193	AV: network	Severity: medium