Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

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-2017-17479	
Vers: 2.3.0-2+deb10u2	Fix: n/a
Name: openjpeg2 Namespace: debian:10 Description: In OpenJPEG 2.3.0, a stack-based buffer overflow was discovered in the pgxtoimage function in jpwl/convert.c. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service or possibly remote code execution.	

CVE-2017-6519	
Vers: 0.7-4+deb10u1	Fix: n/a
Name: avahi Namespace: debian:10 Description: 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.	

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	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

over-read in bmp2tiff.

CVE-2018-12699	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: 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.	

CVE-2018-7648	
Vers: 2.3.0-2+deb10u2	Fix: n/a
Name: openjpeg2 Namespace: debian:10 Description: 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.	

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."	

CVE-2019-13224	
Vers: 6.9.1-1	Fix: n/a
Name: libonig Namespace: debian:10 Description: A use-after-free in onig_new_deluxe() in regext.c in Oniguruma 6.9.2 allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression. The attacker provides a pair of a regex pattern and a string, with a	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

multi-byte encoding that gets handled by onig_new_deluxe(). Oniguruma issues often affect Ruby, as well as common optional libraries for PHP and Rust.

CVE-2019-19012	
Vers: 6.9.1-1	Fix: n/a
Name: libonig Namespace: debian:10 Description: An integer overflow in the search_in_range function in regexec.c in Oniguruma 6.x before 6.9.4_rc2 leads to an out-of-bounds read, in which the offset of this read is under the control of an attacker. (This only affects the 32-bit compiled version). Remote attackers can cause a denial-of-service or information disclosure, or possibly have unspecified other impact, via a crafted regular expression.	

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-2020-11656	
Vers: 3.27.2-3+deb10u1	Fix: n/a
Name: sqlite3 Namespace: debian:10 Description: In SQLite through 3.31.1, the ALTER TABLE implementation has a use-after-free, as demonstrated by an ORDER BY clause that belongs to a compound SELECT statement.	

CVE-2020-12268	
Vers: 0.16-1	Fix: n/a
Name: jbig2dec Namespace: debian:10 Description: jbig2_image_compose in jbig2_image.c in Artifex jbig2dec before 0.18 has a heap-based buffer overflow.	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

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.	

CVE-2021-35942	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 Description: The wordexp function in the GNU C Library (aka glibc) through 2.33 may crash or read arbitrary memory in parse_param (in posix/wordexp.c) when called with an untrusted, crafted pattern, potentially resulting in a denial of service or disclosure of information. This occurs because atoi was used but strtoul should have been used to ensure correct calculations.	

Attack Vector: Network, Severity: High

CVE-2007-0086	
Vers: 2.4.38-3+deb10u5	Fix: n/a
Name: apache2 Namespace: debian:10 Description: ** DISPUTED ** The Apache HTTP Server, when accessed through a TCP connection with a large window size, allows remote attackers to cause a denial of service (network bandwidth consumption) via a Range header that specifies multiple copies of the same fragment. NOTE: the severity of this issue has been disputed by third parties, who state that the large window size required by the attack is not normally supported or configured by the server, or that a DDoS-style attack would accomplish the same goal.	

CVE-2008-1687	
Vers: 1.4.18-2	Fix: n/a

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

Name: m4 Namespace: debian:10 Description: 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.

CVE-2008-1688	
Vers: 1.4.18-2	Fix: n/a
Name: m4 Namespace: debian:10 Description: 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.	

CVE-2008-4609	
Vers: 4.19.194-3	Fix: n/a
Name: linux Namespace: debian:10 Description: 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.	

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-2013-7445	
Vers: 4.19.194-3	Fix: n/a
Name: linux Namespace: debian:10 Description: The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

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.

CVE-2014-8166	
Vers: 2.2.10-6+deb10u4	Fix: n/a
Name: cups Namespace: debian:10 Description: The browsing feature in the server in CUPS does not filter ANSI escape sequences from shared printer names, which might allow remote attackers to execute arbitrary code via a crafted printer name.	

CVE-2016-9113	
Vers: 2.3.0-2+deb10u2	Fix: n/a
Name: openjpeg2 Namespace: debian:10 Description: There is a NULL pointer dereference in function imagetobmp of convertbmp.c:980 of OpenJPEG 2.1.2. image->comps[0].data is not assigned a value after initialization(NULL). Impact is Denial of Service.	

CVE-2016-9114	
Vers: 2.3.0-2+deb10u2	Fix: n/a
Name: openjpeg2 Namespace: debian:10 Description: There is a NULL Pointer Access in function imagetopnm of convert.c:1943(jp2) of OpenJPEG 2.1.2. image->comps[compno].data is not assigned a value after initialization(NULL). Impact is Denial of Service.	

CVE-2016-9580	
Vers: 2.3.0-2+deb10u2	Fix: n/a
Name: openjpeg2 Namespace: debian:10 Description: An integer overflow vulnerability was found in tiftoimage function in openjpeg 2.1.2,	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

resulting in heap buffer overflow.

CVE-2016-9581	
Vers: 2.3.0-2+deb10u2	Fix: n/a
Name: openjpeg2 Namespace: debian:10 Description: An infinite loop vulnerability in tiftoimage that results in heap buffer overflow in convert_32s_C1P1 was found in openjpeg 2.1.2.	

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	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

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 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-2017-7245	
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: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

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-2018-12697	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: 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.	

CVE-2018-12698	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: 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.	

CVE-2018-12700	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: 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.	

CVE-2018-12886	
Vers: 8.3.0-6	Fix: n/a

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

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-2018-12934	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: 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.	

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-2018-16375	
Vers: 2.3.0-2+deb10u2	Fix: n/a
Name: openjpeg2 Namespace: debian:10 Description: An issue was discovered in OpenJPEG 2.3.0. Missing checks for header_info.height and header_info.width in the function pnmtoimage in bin/jpwl/convert.c can lead to a heap-based buffer overflow.	

CVE-2018-16376	
Vers: 2.3.0-2+deb10u2	Fix: n/a

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

Name: openjpeg2 Namespace: debian:10 Description: An issue was discovered in OpenJPEG 2.3.0. A heap-based buffer overflow was discovered in the function t2_encode_packet in lib/openmj2/t2.c. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service or possibly unspecified other impact.

CVE-2018-18483	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: The get_count function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31, allows remote attackers to cause a denial of service (malloc called with the result of an integer-overflowing calculation) or possibly have unspecified other impact via a crafted string, as demonstrated by c++filt.	

CVE-2018-19931	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: 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.	

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+deb10u2	Fix: n/a
Name: krb5	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

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-2018-6951	
Vers: 2.7.6-3+deb10u1	Fix: n/a
Name: patch Namespace: debian:10 Description: 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.	

CVE-2018-6952	
Vers: 2.7.6-3+deb10u1	Fix: n/a
Name: patch Namespace: debian:10 Description: A double free exists in the another_hunk function in pch.c in GNU patch through 2.7.6.	

CVE-2019-1010023	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

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 bug and no real threat."

CVE-2019-1010180	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: GNU gdb All versions is affected by: Buffer Overflow - Out of bound memory access. The impact is: Deny of Service, Memory Disclosure, and Possible Code Execution. The component is: The main gdb module. The attack vector is: Open an ELF for debugging. The fixed version is: Not fixed yet.	

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-2019-12615	
Vers: 4.19.194-3	Fix: n/a
Name: linux Namespace: debian:10 Description: 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).	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

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	
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-2019-16163	
Vers: 6.9.1-1	Fix: n/a
Name: libonig Namespace: debian:10	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

Description: Oniguruma before 6.9.3 allows Stack Exhaustion in regcomp.c because of recursion in regparse.c.

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-2019-19064	
Vers: 4.19.194-3	Fix: n/a
Name: linux Namespace: debian:10 Description: ** DISPUTED ** A memory leak in the fsl_lpspi_probe() function in drivers/spi/spi-fsl-lpspi.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering pm_runtime_get_sync() failures, aka CID-057b8945f78f. NOTE: third parties dispute the relevance of this because an attacker cannot realistically control these failures at probe time.	

CVE-2019-19070	
Vers: 4.19.194-3	Fix: n/a

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

Name: linux Namespace: debian:10 Description: ** DISPUTED ** A memory leak in the spi_gpio_probe() function in drivers/spi/spi-gpio.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering devm_add_action_or_reset() failures, aka CID-d3b0ffa1d75d. NOTE: third parties dispute the relevance of this because the system must have already been out of memory before the probe began.

CVE-2019-19203	
Vers: 6.9.1-1	Fix: n/a
Name: libonig Namespace: debian:10 Description: An issue was discovered in Oniguruma 6.x before 6.9.4_rc2. In the function gb18030_mbc_enc_len in file gb18030.c, a UChar pointer is dereferenced without checking if it passed the end of the matched string. This leads to a heap-based buffer over-read.	

CVE-2019-19204	
Vers: 6.9.1-1	Fix: n/a
Name: libonig Namespace: debian:10 Description: An issue was discovered in Oniguruma 6.x before 6.9.4_rc2. In the function fetch_interval_quantifier (formerly known as fetch_range_quantifier) in regparse.c, PFETCH is called without checking PEND. This leads to a heap-based buffer over-read.	

CVE-2019-19244	
Vers: 3.27.2-3+deb10u1	Fix: n/a
Name: sqlite3 Namespace: debian:10 Description: sqlite3Select in select.c in SQLite 3.30.1 allows a crash if a sub-select uses both DISTINCT and window functions, and also has certain ORDER BY usage.	

CVE-2019-19246	
Vers: 6.9.1-1	Fix: n/a
Name: libonig	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

Namespace: debian:10 Description: Oniguruma through 6.9.3, as used in PHP 7.3.x and other products, has a heap-based buffer over-read in str_lower_case_match in regexec.c.

CVE-2019-19378	
Vers: 4.19.194-3	Fix: n/a
Name: linux Namespace: debian:10 Description: In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image can lead to slab-out-of-bounds write access in index_rbio_pages in fs/btrfs/raid56.c.	

CVE-2019-19449	
Vers: 4.19.194-3	Fix: n/a
Name: linux Namespace: debian:10 Description: In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can lead to slab-out-of-bounds read access in f2fs_build_segment_manager in fs/f2fs/segment.c, related to init_min_max_mtime in fs/f2fs/segment.c (because the second argument to get_seg_entry is not validated).	

CVE-2019-19603	
Vers: 3.27.2-3+deb10u1	Fix: n/a
Name: sqlite3 Namespace: debian:10 Description: SQLite 3.30.1 mishandles certain SELECT statements with a nonexistent VIEW, leading to an application crash.	

CVE-2019-19814	
Vers: 4.19.194-3	Fix: n/a
Name: linux Namespace: debian:10 Description: In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause __remove_dirty_segment slab-out-of-bounds write access because an array is bounded by the number of dirty types (8) but the array index can exceed this.	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

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.	

CVE-2019-9070	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: 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.	

CVE-2019-9075	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: 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.	

CVE-2019-9077	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: 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.	

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,	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

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-2020-19498	
Vers: 1.3.2-2~deb10u1	Fix: n/a
Name: libheif Namespace: debian:10 Description: Floating point exception in function Fraction in libheif 1.4.0, allows attackers to cause a Denial of Service or possibly other unspecified impacts.	

CVE-2020-19499	
Vers: 1.3.2-2~deb10u1	Fix: n/a
Name: libheif Namespace: debian:10 Description: An issue was discovered in heif::Box_iref::get_references in libheif 1.4.0, allows attackers to cause a Denial of Service or possibly other unspecified impact due to an invalid memory read.	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

CVE-2020-19667	
Vers: 8:6.9.10.23+dfsg-2.1+deb10u1	Fix: n/a
Name: imagemagick Namespace: debian:10 Description: Stack-based buffer overflow and unconditional jump in ReadXPMImage in coders/xpm.c in ImageMagick 7.0.10-7.	

CVE-2020-27752	
Vers: 8:6.9.10.23+dfsg-2.1+deb10u1	Fix: n/a
Name: imagemagick Namespace: debian:10 Description: A flaw was found in ImageMagick in MagickCore/quantum-private.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger a heap buffer overflow. This would most likely lead to an impact to application availability, but could potentially lead to an impact to data integrity as well. This flaw affects ImageMagick versions prior to 7.0.9-0.	

CVE-2020-27766	
Vers: 8:6.9.10.23+dfsg-2.1+deb10u1	Fix: n/a
Name: imagemagick Namespace: debian:10 Description: A flaw was found in ImageMagick in MagickCore/statistic.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned long`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.8-69.	

CVE-2020-29599	
Vers: 8:6.9.10.23+dfsg-2.1+deb10u1	Fix: n/a
Name: imagemagick Namespace: debian:10 Description: ImageMagick before 6.9.11-40 and 7.x before 7.0.10-40 mishandles the -authenticate option, which allows setting a password for password-protected PDF files. The user-controlled password was not properly escaped/sanitized and it was therefore possible to inject additional shell commands via coders/pdf.c.	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

CVE-2020-36325	
Vers: 2.12-1	Fix: n/a
Name: jansson Namespace: debian:10 Description: ** DISPUTED ** An issue was discovered in Jansson through 2.13.1. Due to a parsing error in json_loads, there's an out-of-bounds read-access bug. NOTE: the vendor reports that this only occurs when a programmer fails to follow the API specification.	

CVE-2020-36385	
Vers: 4.19.194-3	Fix: n/a
Name: linux Namespace: debian:10 Description: An issue was discovered in the Linux kernel before 5.10. drivers/infiniband/core/ucma.c has a use-after-free because the ctx is reached via the ctx_list in some ucma_migrate_id situations where ucma_close is called, aka CID-f5449e74802c.	

CVE-2020-6096	
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 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-2021-20294	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: A flaw was found in binutils readelf 2.35 program. An attacker who is able to convince a	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

victim using readelf to read a crafted file could trigger a stack buffer overflow, out-of-bounds write of arbitrary data supplied by the attacker. The highest impact of this flaw is to confidentiality, integrity, and availability.

CVE-2021-20309	
Vers: 8:6.9.10.23+dfsg-2.1+deb10u1	Fix: n/a
Name: imagemagick Namespace: debian:10 Description: A flaw was found in ImageMagick in versions before 7.0.11 and before 6.9.12, where a division by zero in WaveImage() of MagickCore/visual-effects.c may trigger undefined behavior via a crafted image file submitted to an application using ImageMagick. The highest threat from this vulnerability is to system availability.	

CVE-2021-20311	
Vers: 8:6.9.10.23+dfsg-2.1+deb10u1	Fix: n/a
Name: imagemagick Namespace: debian:10 Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGBTransformImage() in the MagickCore/colorspace.c may trigger undefined behavior via a crafted image file that is submitted by an attacker processed by an application using ImageMagick. The highest threat from this vulnerability is to system availability.	

CVE-2021-20312	
Vers: 8:6.9.10.23+dfsg-2.1+deb10u1	Fix: n/a
Name: imagemagick Namespace: debian:10 Description: A flaw was found in ImageMagick in versions 7.0.11, where an integer overflow in WriteTHUMBNAILImage of coders/thumbnail.c may trigger undefined behavior via a crafted image file that is submitted by an attacker and processed by an application using ImageMagick. The highest threat from this vulnerability is to system availability.	

CVE-2021-20313	
Vers: 8:6.9.10.23+dfsg-2.1+deb10u1	Fix: n/a
Name: imagemagick	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

Namespace: debian:10 Description: A flaw was found in ImageMagick in versions before 7.0.11. A potential cipher leak when the calculate signatures in TransformSignature is possible. The highest threat from this vulnerability is to data confidentiality.

CVE-2021-22922	
Vers: 7.64.0-4+deb10u2	Fix: n/a
Name: curl Namespace: debian:10 Description: When curl is instructed to download content using the metalink feature, thecontents is verified against a hash provided in the metalink XML file.The metalink XML file points out to the client how to get the same contentfrom a set of different URLs, potentially hosted by different servers and theclient can then download the file from one or several of them. In a serial orparallel manner.If one of the servers hosting the contents has been breached and the contentsof the specific file on that server is replaced with a modified payload, curlshould detect this when the hash of the file mismatches after a completeddownload. It should remove the contents and instead try getting the contentsfrom another URL. This is not done, and instead such a hash mismatch is onlymentioned in text and the potentially malicious content is kept in the file ondisk.	

CVE-2021-22924	
Vers: 7.64.0-4+deb10u2	Fix: n/a
Name: curl Namespace: debian:10 Description: libcurl keeps previously used connections in a connection pool for subsequenttransfers to reuse, if one of them matches the setup.Due to errors in the logic, the config matching function did not take 'issuercert' into account and it compared the involved paths *case insensitively*,which could lead to libcurl reusing wrong connections.File paths are, or can be, case sensitive on many systems but not all, and caneven vary depending on used file systems.The comparison also didn't include the 'issuer cert' which a transfer can setto qualify how to verify the server certificate.	

CVE-2021-30535	
Vers: 63.1-6+deb10u1	Fix: n/a
Name: icu Namespace: debian:10	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

Description: Double free in ICU in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

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.	

CVE-2021-34183	
Vers: 8:6.9.10.23+dfsg-2.1+deb10u1	Fix: n/a
Name: imagemagick Namespace: debian:10 Description: ImageMagick 7.0.11-14 has a memory leak in AcquireSemaphoreMemory in semaphore.c and AcquireMagickMemory in memory.c.	

CVE-2021-3530	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: A flaw was discovered in GNU libiberty within demangle_path() in rust-demangle.c, as distributed in GNU Binutils version 2.36. A crafted symbol can cause stack memory to be exhausted leading to a crash.	

CVE-2021-3549	
Vers: 2.31.1-16	Fix: n/a
Name: binutils Namespace: debian:10 Description: An out of bounds flaw was found in GNU binutils objdump utility version 2.36. An attacker could use this flaw and pass a large section to avr_elf32_load_records_from_section() probably resulting in a crash or in some cases memory corruption. The highest threat from this vulnerability is to integrity as well as system availability.	

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

CVE-2021-38207	
Vers: 4.19.194-3	Fix: n/a
Name: linux Namespace: debian:10 Description: drivers/net/ethernet/xilinx/ll_temac_main.c in the Linux kernel before 5.12.13 allows remote attackers to cause a denial of service (buffer overflow and lockup) by sending heavy network traffic for about ten minutes.	

Additional Findings

CVE-2003-1307	AV: local	Severity: medium
CVE-2003-1580	AV: network	Severity: medium
CVE-2004-0230	AV: network	Severity: medium
CVE-2005-3660	AV: local	Severity: medium
CVE-2007-1743	AV: local	Severity: medium
CVE-2007-3303	AV: local	Severity: medium
CVE-2007-5686	AV: local	Severity: medium
CVE-2007-6755	AV: network	Severity: medium
CVE-2008-2544	AV: local	Severity: medium
CVE-2008-3134	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-2010-4563	AV: network	Severity: medium
CVE-2010-4651	AV: network	Severity: medium
CVE-2010-4756	AV: network	Severity: medium
CVE-2010-5321	AV: local	Severity: medium
CVE-2011-3389	AV: network	Severity: medium
CVE-2011-4915	AV: local	Severity: medium
CVE-2012-0039	AV: network	Severity: medium
CVE-2012-4542	AV: local	Severity: medium
CVE-2013-0340	AV: network	Severity: medium
CVE-2013-4235	AV: local	Severity: medium

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

CVE-2014-8130	AV: network	Severity: medium
CVE-2014-9892	AV: network	Severity: medium
CVE-2014-9900	AV: network	Severity: medium
CVE-2015-3276	AV: network	Severity: medium
CVE-2016-10228	AV: network	Severity: medium
CVE-2016-10505	AV: network	Severity: medium
CVE-2016-10506	AV: network	Severity: medium
CVE-2016-10723	AV: local	Severity: medium
CVE-2016-2781	AV: local	Severity: medium
CVE-2016-8660	AV: local	Severity: medium
CVE-2016-8678	AV: network	Severity: medium
CVE-2016-9115	AV: network	Severity: medium
CVE-2016-9116	AV: network	Severity: medium
CVE-2016-9117	AV: network	Severity: medium
CVE-2016-9318	AV: network	Severity: medium
CVE-2017-0630	AV: network	Severity: medium
CVE-2017-11754	AV: network	Severity: medium
CVE-2017-11755	AV: network	Severity: medium
CVE-2017-13693	AV: local	Severity: medium
CVE-2017-13694	AV: local	Severity: medium
CVE-2017-13716	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-2017-7275	AV: network	Severity: medium
CVE-2017-9937	AV: network	Severity: medium
CVE-2018-1000654	AV: network	Severity: medium
CVE-2018-1000876	AV: local	Severity: high
CVE-2018-10126	AV: network	Severity: medium
CVE-2018-1121	AV: network	Severity: medium
CVE-2018-12928	AV: local	Severity: medium
CVE-2018-14048	AV: network	Severity: medium
CVE-2018-15607	AV: network	Severity: medium

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

CVE-2018-17358	AV: network	Severity: medium
CVE-2018-17359	AV: network	Severity: medium
CVE-2018-17360	AV: network	Severity: medium
CVE-2018-17794	AV: network	Severity: medium
CVE-2018-17977	AV: local	Severity: medium
CVE-2018-17985	AV: network	Severity: medium
CVE-2018-18309	AV: network	Severity: medium
CVE-2018-18484	AV: network	Severity: medium
CVE-2018-18605	AV: network	Severity: medium
CVE-2018-18606	AV: network	Severity: medium
CVE-2018-18607	AV: network	Severity: medium
CVE-2018-18700	AV: network	Severity: medium
CVE-2018-18701	AV: network	Severity: medium
CVE-2018-19932	AV: network	Severity: medium
CVE-2018-20002	AV: network	Severity: medium
CVE-2018-20623	AV: network	Severity: medium
CVE-2018-20651	AV: network	Severity: medium
CVE-2018-20671	AV: network	Severity: medium
CVE-2018-20673	AV: network	Severity: medium
CVE-2018-20712	AV: network	Severity: medium
CVE-2018-20845	AV: network	Severity: medium
CVE-2018-20846	AV: network	Severity: medium
CVE-2018-21232	AV: network	Severity: medium
CVE-2018-5727	AV: network	Severity: medium
CVE-2018-7169	AV: network	Severity: medium
CVE-2018-9138	AV: network	Severity: medium
CVE-2018-9996	AV: network	Severity: medium
CVE-2019-1010024	AV: network	Severity: medium
CVE-2019-1010025	AV: network	Severity: medium
CVE-2019-1010204	AV: network	Severity: medium
CVE-2019-12378	AV: local	Severity: medium
CVE-2019-12379	AV: local	Severity: medium
CVE-2019-12380	AV: local	Severity: medium
CVE-2019-12381	AV: local	Severity: medium

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

CVE-2019-12382	AV: local	Severity: medium
CVE-2019-12455	AV: local	Severity: medium
CVE-2019-12456	AV: local	Severity: high
CVE-2019-12972	AV: network	Severity: medium
CVE-2019-12973	AV: network	Severity: medium
CVE-2019-13225	AV: network	Severity: medium
CVE-2019-13310	AV: network	Severity: medium
CVE-2019-13627	AV: local	Severity: medium
CVE-2019-14250	AV: network	Severity: medium
CVE-2019-14444	AV: network	Severity: medium
CVE-2019-15213	AV: local	Severity: medium
CVE-2019-15794	AV: local	Severity: medium
CVE-2019-16089	AV: local	Severity: medium
CVE-2019-16229	AV: local	Severity: medium
CVE-2019-16230	AV: local	Severity: medium
CVE-2019-16231	AV: local	Severity: medium
CVE-2019-16232	AV: local	Severity: medium
CVE-2019-16233	AV: local	Severity: medium
CVE-2019-16234	AV: local	Severity: medium
CVE-2019-16709	AV: network	Severity: medium
CVE-2019-17450	AV: network	Severity: medium
CVE-2019-17451	AV: network	Severity: medium
CVE-2019-17567	AV: network	Severity: medium
CVE-2019-18276	AV: local	Severity: high
CVE-2019-19083	AV: local	Severity: medium
CVE-2019-19645	AV: local	Severity: medium
CVE-2019-19882	AV: local	Severity: high
CVE-2019-19924	AV: network	Severity: medium
CVE-2019-20794	AV: local	Severity: medium
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-2019-6988	AV: network	Severity: medium

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

CVE-2019-9071	AV: network	Severity: medium
CVE-2019-9073	AV: network	Severity: medium
CVE-2019-9074	AV: network	Severity: medium
CVE-2020-10001	AV: network	Severity: medium
CVE-2020-10029	AV: local	Severity: medium
CVE-2020-10251	AV: network	Severity: medium
CVE-2020-11725	AV: local	Severity: high
CVE-2020-12362	AV: local	Severity: high
CVE-2020-12363	AV: local	Severity: medium
CVE-2020-12364	AV: local	Severity: medium
CVE-2020-13529	AV: local	Severity: medium
CVE-2020-13631	AV: local	Severity: medium
CVE-2020-13776	AV: local	Severity: medium
CVE-2020-14155	AV: network	Severity: medium
CVE-2020-14304	AV: local	Severity: medium
CVE-2020-15719	AV: network	Severity: medium
CVE-2020-15802	AV: network	Severity: medium
CVE-2020-16119	AV: local	Severity: high
CVE-2020-16120	AV: local	Severity: medium
CVE-2020-16590	AV: network	Severity: medium
CVE-2020-16591	AV: network	Severity: medium
CVE-2020-16592	AV: network	Severity: medium
CVE-2020-16593	AV: network	Severity: medium
CVE-2020-16599	AV: network	Severity: medium
CVE-2020-1751	AV: local	Severity: high
CVE-2020-1752	AV: local	Severity: high
CVE-2020-25664	AV: network	Severity: medium
CVE-2020-25665	AV: network	Severity: medium
CVE-2020-25674	AV: network	Severity: medium
CVE-2020-25676	AV: network	Severity: medium
CVE-2020-26141	AV: local	Severity: medium
CVE-2020-26145	AV: local	Severity: medium
CVE-2020-26541	AV: local	Severity: medium
CVE-2020-26555	AV: local	Severity: medium

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

CVE-2020-26556	AV: local	Severity: high
CVE-2020-26557	AV: local	Severity: high
CVE-2020-26559	AV: local	Severity: high
CVE-2020-26560	AV: local	Severity: high
CVE-2020-27618	AV: local	Severity: medium
CVE-2020-27750	AV: network	Severity: medium
CVE-2020-27753	AV: network	Severity: medium
CVE-2020-27756	AV: network	Severity: medium
CVE-2020-27760	AV: network	Severity: medium
CVE-2020-27762	AV: network	Severity: medium
CVE-2020-27770	AV: network	Severity: medium
CVE-2020-27835	AV: local	Severity: medium
CVE-2020-35457	AV: local	Severity: high
CVE-2020-35493	AV: network	Severity: medium
CVE-2020-35494	AV: network	Severity: medium
CVE-2020-35495	AV: network	Severity: medium
CVE-2020-35496	AV: network	Severity: medium
CVE-2020-35507	AV: network	Severity: medium
CVE-2020-35521	AV: network	Severity: medium
CVE-2020-35522	AV: network	Severity: medium
CVE-2020-36310	AV: local	Severity: medium
CVE-2020-36322	AV: local	Severity: medium
CVE-2021-20176	AV: network	Severity: medium
CVE-2021-20193	AV: network	Severity: medium
CVE-2021-20197	AV: local	Severity: medium
CVE-2021-20241	AV: network	Severity: medium
CVE-2021-20243	AV: network	Severity: medium
CVE-2021-20244	AV: network	Severity: medium
CVE-2021-20245	AV: network	Severity: medium
CVE-2021-20246	AV: network	Severity: medium
CVE-2021-20284	AV: network	Severity: medium
CVE-2021-22543	AV: local	Severity: high
CVE-2021-22923	AV: network	Severity: medium
CVE-2021-26934	AV: local	Severity: high

Scan Report: wordpress:latest

Scan ID: ff71f9f5-d9cd-4352-9dfe-a1427d9b4ca0
Scan requested at: 2021-08-18T18:24:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 14, high - 109, medium - 190

CVE-2021-28950	AV: local	Severity: medium
CVE-2021-29338	AV: network	Severity: medium
CVE-2021-32078	AV: local	Severity: high
CVE-2021-33193	AV: local	Severity: unknown
CVE-2021-33624	AV: local	Severity: medium
CVE-2021-3444	AV: local	Severity: high
CVE-2021-34556	AV: local	Severity: medium
CVE-2021-3468	AV: local	Severity: medium
CVE-2021-3487	AV: network	Severity: medium
CVE-2021-3493	AV: local	Severity: high
CVE-2021-35039	AV: local	Severity: high
CVE-2021-3542	AV: local	Severity: unknown
CVE-2021-35477	AV: local	Severity: medium
CVE-2021-3575	AV: local	Severity: unknown
CVE-2021-3600	AV: local	Severity: unknown
CVE-2021-3612	AV: local	Severity: high
CVE-2021-3635	AV: local	Severity: unknown
CVE-2021-3640	AV: local	Severity: unknown
CVE-2021-3653	AV: local	Severity: unknown
CVE-2021-3669	AV: local	Severity: unknown
CVE-2021-3679	AV: local	Severity: medium
CVE-2021-37159	AV: local	Severity: medium
CVE-2021-37576	AV: local	Severity: high
CVE-2021-37600	AV: local	Severity: medium
CVE-2021-38160	AV: local	Severity: high
CVE-2021-38198	AV: local	Severity: medium
CVE-2021-38199	AV: local	Severity: medium
CVE-2021-38203	AV: local	Severity: medium
CVE-2021-38204	AV: local	Severity: medium
CVE-2021-38206	AV: local	Severity: medium