Deep Security
Smart Check

Scan Report: python:latest

Scan ID: 20442136-39de-4ab6-a9b8-0b04d32d08f0
Scan requested at: 2021-08-18T18:28:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 11, high - 62, medium - 129

Attack Vector: Network, Severity: Critical

CVE-2005-2541	
Vers: 1.34+dfsg-1	Fix: n/a
Name: tar Namespace: debian:11 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-2009-3546	
Vers: 0.2.8.4-17	Fix: n/a
Name: libwmf Namespace: debian:11 Description: The _gdGetColors function in gd_gd.c in PHP 5.2.11 and 5.3.x before 5.3.1, and the GD Graphics Library 2.x, does not properly verify a certain colorsTotal structure member, which might allow remote attackers to conduct buffer overflow or buffer over-read attacks via a crafted GD file, a different vulnerability than CVE-2009-3293. NOTE: some of these details are obtained from third party information.	

CVE-2017-17479	
Vers: 2.4.0-3	Fix: n/a
Name: openjpeg2 Namespace: debian:11 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-2017-9117	
Vers: 4.2.0-1	Fix: n/a
Name: tiff Namespace: debian:11 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-2019-1010022	
Vers: 2.31-13	Fix: n/a
Name: glibc Namespace: debian:11 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-2020-27619	
Vers: 3.9.2-1	Fix: n/a
Name: python3.9 Namespace: debian:11 Description: In Python 3 through 3.9.0, the Lib/test/multibytecodec_support.py CJK codec tests call eval() on content retrieved via HTTP.	

CVE-2021-29921	
Vers: 3.9.2-1	Fix: n/a
Name: python3.9 Namespace: debian:11 Description: In Python before 3,9,5, the ipaddress library mishandles leading zero characters in the octets of an IP address string. This (in some situations) allows attackers to bypass access control that is based on IP addresses.	

CVE-2021-30473	
Vers: 1.0.0.errata1-3	Fix: n/a
Name: aom Namespace: debian:11 Description: aom_image.c in libaom in AOMedia before 2021-04-07 frees memory that is not located on the heap.	

CVE-2021-30474

Vers: 1.0.0.errata1-3	Fix: n/a
Name: aom Namespace: debian:11 Description: aom_dsp/grain_table.c in libaom in AOMedia before 2021-03-30 has a use-after-free.	

CVE-2021-30475	
Vers: 1.0.0.errata1-3	Fix: n/a
Name: aom Namespace: debian:11 Description: aom_dsp/noise_model.c in libaom in AOMedia before 2021-03-24 has a buffer overflow.	

CVE-2021-33574	
Vers: 2.31-13	Fix: n/a
Name: glibc Namespace: debian:11 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-2008-1687	
Vers: 1.4.18-5	Fix: n/a
Name: m4 Namespace: debian:11 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: 1.4.18-5	Fix: n/a

Scan Report: python:latest

Scan ID: 20442136-39de-4ab6-a9b8-0b04d32d08f0
Scan requested at: 2021-08-18T18:28:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 11, high - 62, medium - 129

Name: m4 Namespace: debian:11 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: 5.10.46-4	Fix: n/a
Name: linux Namespace: debian:11 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: 5.32.1-4+deb11u1	Fix: n/a
Name: perl Namespace: debian:11 Description: _is_safe in the File::Temp module for Perl does not properly handle symlinks.	

CVE-2013-7445	
Vers: 5.10.46-4	Fix: n/a
Name: linux Namespace: debian:11 Description: 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.	

CVE-2016-9113	
Vers: 2.4.0-3	Fix: n/a
Name: openjpeg2	

Namespace: debian:11 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: 2.4.0-3	Fix: n/a
Name: openjpeg2 Namespace: debian:11 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: 2.4.0-3	Fix: n/a
Name: openjpeg2 Namespace: debian:11 Description: An integer overflow vulnerability was found in tiftoimage function in openjpeg 2.1.2, resulting in heap buffer overflow.	

CVE-2016-9581	
Vers: 2.4.0-3	Fix: n/a
Name: openjpeg2 Namespace: debian:11 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-2016-9917	
Vers: 5.55-3.1	Fix: n/a
Name: bluez Namespace: debian:11 Description: In BlueZ 5.42, a buffer overflow was observed in "read_n" function in "tools/hcidump.c" source file. This issue can be triggered by processing a corrupted dump file and will result in hcidump crash.	

Scan Report: python:latest

Scan ID: 20442136-39de-4ab6-a9b8-0b04d32d08f0
Scan requested at: 2021-08-18T18:28:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 11, high - 62, medium - 129

CVE-2016-9918	
Vers: 5.55-3.1	Fix: n/a
Name: bluez Namespace: debian:11 Description: In BlueZ 5.42, an out-of-bounds read was identified in "packet_hexdump" function in "monitor/packet.c" source file. This issue can be triggered by processing a corrupted dump file and will result in btmon crash.	

CVE-2017-11164	
Vers: 2:8.39-13	Fix: n/a
Name: pcre3 Namespace: debian:11 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: 4.2.0-1	Fix: n/a
Name: tiff Namespace: debian:11 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-2017-17740	
Vers: 2.4.57+dfsg-3	Fix: n/a
Name: openldap Namespace: debian:11 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: 4.2.0-1	Fix: n/a

Name: tiff Namespace: debian:11 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: 4.2.0-1	Fix: n/a
Name: tiff Namespace: debian:11 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: 2:8.39-13	Fix: n/a
Name: pcre3 Namespace: debian:11 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: 2:8.39-13	Fix: n/a
Name: pcre3 Namespace: debian:11 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 possibly have unspecified other impact via a crafted file.	

CVE-2017-9814	
Vers: 1.16.0-5	Fix: n/a
Name: cairo Namespace: debian:11 Description: 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.

CVE-2018-1000021	
Vers: 1:2.30.2-1	Fix: n/a
Name: git Namespace: debian:11 Description: 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).	

CVE-2018-12934	
Vers: 2.35.2-2	Fix: n/a
Name: binutils Namespace: debian:11 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-2018-16375	
Vers: 2.4.0-3	Fix: n/a
Name: openjpeg2 Namespace: debian:11 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: 2.4.0-3	Fix: n/a
Name: openjpeg2 Namespace: debian:11 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: 2.35.2-2

Fix: n/a

Name: binutils

Namespace: debian:11

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-2018-20796

Vers: 2.31-13

Fix: n/a

Name: glibc

Namespace: debian:11

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: 1.18.3-6

Fix: n/a

Name: krb5

Namespace: debian:11

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: 1.8.7-6

Fix: n/a

Name: libgcrypt20

Namespace: debian:11

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: 2.7.6-7	Fix: n/a
Name: patch Namespace: debian:11 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: 2.7.6-7	Fix: n/a
Name: patch Namespace: debian:11 Description: A double free exists in the another_hunk function in pch.c in GNU patch through 2.7.6.	

CVE-2019-1010023	
Vers: 2.31-13	Fix: n/a
Name: glibc Namespace: debian:11 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-2019-19070	
Vers: 5.10.46-4	Fix: n/a
Name: linux Namespace: debian:11 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-2019-19378	
Vers: 5.10.46-4	Fix: n/a
Name: linux Namespace: debian:11 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: 5.10.46-4	Fix: n/a
Name: linux Namespace: debian:11 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-2019-19814	
Vers: 5.10.46-4	Fix: n/a
Name: linux Namespace: debian:11 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.	

CVE-2019-20838	
Vers: 2:8.39-13	Fix: n/a
Name: pcre3 Namespace: debian:11 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: python:latest

Scan ID: 20442136-39de-4ab6-a9b8-0b04d32d08f0
Scan requested at: 2021-08-18T18:28:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 11, high - 62, medium - 129

CVE-2019-9192	
Vers: 2.31-13	Fix: n/a
Name: glibc Namespace: debian:11 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-2020-15778	
Vers: 1:8.4p1-5	Fix: n/a
Name: openssh Namespace: debian:11 Description: ** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."	

CVE-2021-20309	
Vers: 8:6.9.11.60+dfsg-1.3	Fix: n/a
Name: imagemagick Namespace: debian:11 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: 8:6.9.11.60+dfsg-1.3	Fix: n/a
Name: imagemagick Namespace: debian:11 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: 8:6.9.11.60+dfsg-1.3	Fix: n/a
Name: imagemagick Namespace: debian:11 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: 8:6.9.11.60+dfsg-1.3	Fix: n/a
Name: imagemagick Namespace: debian:11 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: 7.74.0-1.3	Fix: n/a
Name: curl Namespace: debian:11 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

Scan Report: python:latest

Scan ID: 20442136-39de-4ab6-a9b8-0b04d32d08f0
Scan requested at: 2021-08-18T18:28:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 11, high - 62, medium - 129

Vers: 7.74.0-1.3	Fix: n/a
Name: curl Namespace: debian:11 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-2021-34183	
Vers: 8:6.9.11.60+dfsg-1.3	Fix: n/a
Name: imagemagick Namespace: debian:11 Description: ImageMagick 7.0.11-14 has a memory leak in AcquireSemaphoreMemory in semaphore.c and AcquireMagickMemory in memory.c.	

CVE-2021-3530	
Vers: 2.35.2-2	Fix: n/a
Name: binutils Namespace: debian:11 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-2021-35331	
Vers: 8.6.11+dfsg-1	Fix: n/a
Name: tcl8.6 Namespace: debian:11 Description: ** DISPUTED ** In Tcl 8.6.11, a format string vulnerability in nmakehlp.c might allow code execution via a crafted file. NOTE: multiple third parties dispute the significance of this finding.	

CVE-2021-3549	
Vers: 2.35.2-2	Fix: n/a

Scan Report: python:latest

Scan ID: 20442136-39de-4ab6-a9b8-0b04d32d08f0
Scan requested at: 2021-08-18T18:28:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 11, high - 62, medium - 129

Name: binutils

Namespace: debian:11

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.

Additional Findings

CVE-2004-0230	AV: network	Severity: medium
CVE-2005-3660	AV: local	Severity: medium
CVE-2007-2243	AV: network	Severity: medium
CVE-2007-2768	AV: network	Severity: medium
CVE-2007-3476	AV: network	Severity: medium
CVE-2007-3477	AV: network	Severity: medium
CVE-2007-3996	AV: network	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-2008-3234	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

Scan Report: python:latest

Scan ID: 20442136-39de-4ab6-a9b8-0b04d32d08f0
Scan requested at: 2021-08-18T18:28:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 11, high - 62, medium - 129

CVE-2013-4235	AV: local	Severity: medium
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-2015-9019	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-2016-9797	AV: network	Severity: medium
CVE-2016-9798	AV: network	Severity: medium
CVE-2016-9799	AV: network	Severity: medium
CVE-2016-9800	AV: network	Severity: medium
CVE-2016-9801	AV: network	Severity: medium
CVE-2016-9802	AV: network	Severity: medium
CVE-2016-9803	AV: network	Severity: medium
CVE-2016-9804	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-2017-14988	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

Scan Report: python:latest

Scan ID: 20442136-39de-4ab6-a9b8-0b04d32d08f0
Scan requested at: 2021-08-18T18:28:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 11, high - 62, medium - 129

CVE-2017-7475	AV: network	Severity: medium
CVE-2017-9937	AV: network	Severity: medium
CVE-2018-10126	AV: network	Severity: medium
CVE-2018-1121	AV: network	Severity: medium
CVE-2018-12928	AV: local	Severity: medium
CVE-2018-15607	AV: network	Severity: medium
CVE-2018-15919	AV: network	Severity: medium
CVE-2018-17977	AV: local	Severity: medium
CVE-2018-18064	AV: network	Severity: medium
CVE-2018-20623	AV: network	Severity: medium
CVE-2018-20673	AV: network	Severity: medium
CVE-2018-20712	AV: network	Severity: medium
CVE-2018-20846	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
CVE-2019-12382	AV: local	Severity: medium
CVE-2019-12455	AV: local	Severity: medium
CVE-2019-12456	AV: local	Severity: high
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-2019-19882	AV: local	Severity: high

Scan Report: python:latest

Scan ID: 20442136-39de-4ab6-a9b8-0b04d32d08f0
Scan requested at: 2021-08-18T18:28:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 11, high - 62, medium - 129

CVE-2019-20794	AV: local	Severity: medium
CVE-2019-6110	AV: network	Severity: medium
CVE-2019-6129	AV: network	Severity: medium
CVE-2019-6461	AV: network	Severity: medium
CVE-2019-6462	AV: network	Severity: medium
CVE-2019-6988	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-2020-14145	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-2020-24504	AV: local	Severity: medium
CVE-2020-26541	AV: local	Severity: medium
CVE-2020-26555	AV: local	Severity: medium
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-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-2021-22923	AV: network	Severity: medium
CVE-2021-23215	AV: network	Severity: medium
CVE-2021-2372	AV: network	Severity: medium
CVE-2021-2389	AV: network	Severity: medium

Scan Report: python:latest

Scan ID: 20442136-39de-4ab6-a9b8-0b04d32d08f0
Scan requested at: 2021-08-18T18:28:15Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 11, high - 62, medium - 129

CVE-2021-26260	AV: network	Severity: medium
CVE-2021-26934	AV: local	Severity: high
CVE-2021-26945	AV: network	Severity: medium
CVE-2021-29338	AV: network	Severity: medium
CVE-2021-31879	AV: network	Severity: medium
CVE-2021-32078	AV: local	Severity: high
CVE-2021-3426	AV: local	Severity: medium
CVE-2021-3487	AV: network	Severity: medium
CVE-2021-35039	AV: local	Severity: high
CVE-2021-3542	AV: local	Severity: unknown
CVE-2021-3575	AV: local	Severity: unknown
CVE-2021-3598	AV: local	Severity: medium
CVE-2021-3605	AV: local	Severity: unknown
CVE-2021-3635	AV: local	Severity: unknown
CVE-2021-3640	AV: local	Severity: unknown
CVE-2021-3653	AV: local	Severity: unknown
CVE-2021-3658	AV: local	Severity: unknown
CVE-2021-3669	AV: local	Severity: unknown
CVE-2021-3677	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-2021-38160	AV: local	Severity: high
CVE-2021-38166	AV: local	Severity: high
CVE-2021-38199	AV: local	Severity: medium
CVE-2021-38203	AV: local	Severity: medium
CVE-2021-38204	AV: local	Severity: medium